WatchGuard® System Manager Fireware Configuration Guide

WatchGuard Fireware™ Pro v8.2

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2005 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the WatchGuard System Manager User Guide. A copy of this book is automatically installed into a subfolder of the installation directory called Documentation. You can also find it online at:
http://www.watchguard.com/help/documentation/

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Guide Version: 8.2-352-2561-001

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

CHAPTER 1 Introduction 1
Fireware Features and Tools 1
Fireware User Interface 2
Policy Manager window 3
Firebox System Manager window 4
CHAPTER 2 Monitoring Firebox Status 7
Starting Firebox System Manager 7
Connecting to a Firebox 7
Opening Firebox System Manager 8
Firebox System Manager Menus and Toolbar 8
Setting refresh interval and pausing the display 10
Seeing Basic Firebox and Network Status 10
Using the Security Traffic Display 10
Monitoring status information 11
Setting the center interface 11
Monitoring traffic, load, and status 12
Firebox and VPN tunnel status 12
Monitoring Firebox Traffic 13
Setting the maximum number of log messages 13
Using color for your log messages 14
Copying log messages 15
Learning more about a traffic log message 15
Clearing the ARP Cache 15
Using the Performance Console 16
Types of counters 16
Defining counters 17
Viewing the performance graph 18
Viewing Bandwidth Usage 19
Viewing Number of Connections by Policy 20

Viewing Information About Firebox Status 22
Status Report 22
Authentication List 23
Blocked Sites 24
Security Services 25
Using HostWatch 26
The HostWatch window 27
Controlling the HostWatch window 28
Changing HostWatch view properties 28
Adding a blocked site from HostWatch 29
Pausing the HostWatch display 29
CHAPTER 3 Setting Up Your Firebox 31
Working with Licenses 31
Adding licenses 32
Deleting a license 32
Seeing the active features 33
Seeing the properties of a license 34
Downloading a license key 34
Working with Aliases 34
Creating an alias 35
Using Logging 35
Categories of log messages 36
Designating log servers for a Firebox 36
Adding a log server 37
Setting log server priority 38
Activating Syslog logging 38
Enabling advanced diagnostics 39
Using Global Settings 39
VPN 40
ICMP error handling 40
TCP SYN checking 41
TCP maximum segment size adjustment 41
Setting NTP Servers 42
Working with SNMP 42
Using MIBs 43
CHAPTER 4 Basic Firebox Configuration 45
Opening a Configuration File 45
Opening a working configuration file 45
Opening a local configuration file 47
Making a new configuration file 47
Saving a Configuration File 47
Saving a configuration to the Firebox 48
Saving a configuration to a local hard drive 48
About Firebox Backup Images 48
Creating a Firebox backup image 48

Restoring a Firebox backup image 49
Changing the Firebox passphrases 49
Setting the Time Zone 50
Setting a Firebox Friendly Name 50
Creating Schedules 50
CHAPTER 5 Network Setup and Configuration 53
Making a New Configuration File 53
Changing Firebox Interface IP Addresses 54
Configuring the external interface 56
Adding Secondary Networks 58
Adding WINS and DNS Server Addresses 60
Configuring Routes 60
Adding a network route 61
Adding a host route 61
Setting Firebox Interface Speed and Duplex 61
CHAPTER 6 Configuring Policies 63
Creating Policies for your Network 63
Adding Policies 64
Changing the Policy Manager View 64
Adding a policy 65
Making a custom policy template 66
Adding more than one policy of the same type 68
Deleting a policy 68
Configuring Policy Properties 68
Setting access rules, sources, and destinations 69
Setting a proxy action 70
Setting logging properties 71
Configuring static NAT 72
Setting advanced properties 74
Setting Policy Precedence 75
Using automatic order 75
Setting precedence manually 77
CHAPTER 7 Configuring Proxied Policies 79
Defining Rules 79
Adding rulesets 80
Using advanced rules view 81
Customizing Logging and Notification for Proxy Rules 82
Configuring log messages and notification for a proxy policy 82
Configuring log messages and alarms for a proxy rule 82
Using dialog boxes for alarms, log messages, and notification 83
Configuring the SMTP Proxy 84
Configuring general settings 85
Configuring ESMTP parameters 86
Configuring authentication rules 87

Defining content type rules 88
Defining file name rules 88
Configuring the Mail From and Mail To rules 88
Defining header rules 88
Defining antivirus responses 88
Changing the deny message 89
Configuring the IPS (Intrusion Prevention System) for SMTP 89
Configuring spamBlocker 89
Configuring proxy and antivirus alarms for SMTP 89
Configuring the FTP Proxy 90
Configuring general settings 90
Defining commands rules for FTP 91
Setting download rules for FTP 91
Setting upload rules for FTP 91
Enabling intrusion prevention for FTP 91
.Configuring proxy alarms for FTP 92
Configuring the HTTP Proxy 92
Configuring settings for HTTP requests 92
Configuring general settings for HTTP responses 95
Setting header fields for HTTP responses 95
Setting content types for HTTP responses 95
Setting cookies for HTTP responses 95
Setting HTTP body content types 96
Changing the deny message 96
Enabling intrusion prevention for HTTP 97
Defining proxy and antivirus alarms for HTTP 98
Configuring the DNS Proxy 98
Configuring general settings for the DNS proxy 98
Configuring DNS OPcodes 99
Configuring DNS query types 100
Configuring DNS query names 101
Enabling intrusion prevention for DNS 101
Configuring DNS proxy alarms 101
Configuring the TCP Proxy 101
Configuring general settings for the TCP proxy 101
Enabling intrusion prevention for TCP 102
CHAPTER 8 Working with Firewall NAT 103
Using Dynamic NAT 104
Adding global dynamic NAT entries 104
Reordering dynamic NAT entries 105
Policy-based dynamic NAT entries 105
Using 1-to-1 NAT 105
Defining a 1-to-1 NAT rule 106
Configuring global 1-to-1 NAT 107
Configuring policy-based 1-to-1 NAT 108
Configuring Static NAT for a Policy 108

CHAPTER 9 Implementing Authentication 111
How User Authentication Works 111
Using authentication from the external network 111
Using authentication through a gateway Firebox to another Firebox 112
Authentication server types 112
Using a backup authentication server 112
Configuring the Firebox as an Authentication Server 113
About Firebox authentication 113
Setting up the Firebox as an authentication server 115
Using a local user account for Firewall user, PPTP and MUVPN authentication 116
Configuring RADIUS Server Authentication 117
Configuring SecurID Authentication 118
Configuring LDAP Authentication 119
Configuring Active Directory Authentication 121
Configuring a Policy with User Authentication 122
CHAPTER 10 Firewall Intrusion Detection and Prevention 125
Using Default Packet Handling Options 125
Spoofing attacks 126
IP source route attacks 126
"Ping of death" attacks 126
Port space and address space attacks 127
Flood attacks 127
Unhandled Packets 127
Distributed denial of service attacks 127
Setting Blocked Sites 127
Blocking a site permanently 128
Using an external list of blocked sites 129
Creating exceptions to the Blocked Sites list 129
Setting logging and notification parameters 129
Blocking sites temporarily with policy settings 130
Blocking Ports 131
Blocking a port permanently 132
Automatically blocking IP addresses that try to use blocked ports 132
Setting logging and notification for blocked ports 132
CHAPTER 11 Using Signature-Based Security Services 133
Installing the Software Licenses 133
Activating Gateway AntiVirus 134
Configuring Gateway AntiVirus 136
Creating alarms or log entries for antivirus responses 137
Configuring GAV engine settings 137
Configuring the GAV signature server 138
Using Gateway AntiVirus with more than one proxy 138
Unlocking an attachment locked by Gateway AntiVirus 138
Getting Gateway AntiVirus Status and Updates 138

Seeing service status 139
Updating signatures manually 139
Updating the antivirus software 139
Activating Intrusion Prevention (IPS) 140
Configuring Intrusion Prevention 141
Configuring intrusion prevention for HTTP or TCP 142
Configuring Intrusion Prevention for FTP, SMTP, or DNS 144
Configuring the signature server 145
Configuring signature exceptions 145
Copying IPS settings to other policies 145
Getting Intrusion Prevention Service Status and Updates 146
Seeing service status 146
Updating signatures manually 147
CHAPTER 12 Introduction to VPNs 149
Tunneling Protocols 150
IPSec 150
PPTP 150
Encryption 150
Selecting an encryption and data integrity method 151
Authentication 151
Extended authentication 151
Selecting an authentication method 151
IP Addressing 152
Internet Key Exchange (IKE) 152
Network Address Translation and VPNs 153
Access Control 153
Network Topology 153
Meshed networks 153
Hub-and-spoke networks 154
Tunneling Methods 155
WatchGuard VPN Solutions 156
Remote User VPN with PPTP 156
Mobile User VPN 156
Branch Office Virtual Private Network (BOVPN) 156
VPN Scenarios 158
Large company with branch offices: System Manager 158
Small company with telecommuters: MUVPN 158
Company with remote employees: MUVPN with extended authentication 159
CHAPTER 13 Configuring BOVPN with Manual IPSec 161
Before You Start 161
Configuring a Gateway 161
Adding a gateway 161
Editing and deleting a gateway 164
Making a Manual Tunnel 164

Editing and deleting a tunnel 167
Making a Tunnel Policy 168
CHAPTER 14 Configuring Managed VPN Tunnels 169
Configuring a Firebox as a Managed Firebox Client 169
Adding Policy Templates 170
Get the current templates from a device 171
Make a new policy template 171
Adding resources to a policy template 172
Adding Security Templates 172
Making Tunnels Between Devices 173
Using the drag-and-drop procedure 173
Using the Add VPN wizard without drag-and-drop 173
Editing a Tunnel 174
Removing Tunnels and Devices 174
Removing a tunnel 174
Removing a device 174
CHAPTER 15 Configuring RUVPN with PPTP 175
Configuration Checklist 175
Encryption levels 175
Configuring WINS and DNS Servers 176
Adding New Users to Authentication Groups 177
Configuring Services to Allow Incoming RUVPN Traffic 178
By individual policy 178
Using the Any policies 178
Enabling RUVPN with PPTP 179
Enabling extended authentication 179
Adding IP Addresses for RUVPN Sessions 179
Preparing the Client Computers 180
Installing MSDUN and Service Packs 180
Creating and Connecting a PPTP RUVPN on Windows XP 181
Creating and Connecting a PPTP RUVPN on Windows 2000 181
Running RUVPN and accessing the Internet 182
Making outbound PPTP connections from behind a Firebox 182
CHAPTER 16 Advanced Networking 183
About Multiple WAN Support 183
Configuring multiple WAN support 185
Creating QoS Actions 186
Applying QoS actions to policies 188
Using QoS in a multiple WAN environment 188
Dynamic Routing 189
Using RIP 189
RIP Version 1 189
RIP Version 2 192

Using OSPF 194
OSPF Daemon Configuration 194
Configuring Fireware to use OSPF 197
Using BGP 198
CHAPTER 17 Controlling Web Site Access with WebBlocker 203
Installing the Software Licenses 203
Getting Started with WebBlocker 204
Automating WebBlocker database downloads 205
Activating WebBlocker 205
Configuring WebBlocker 208
Adding new servers 209
Selecting categories to block 209
Defining WebBlocker exceptions 209
Defining advanced WebBlocker options 211
Scheduling a WebBlocker Action 211
CHAPTER 18 High Availability 213
High Availability Requirements 213
Installing High Availability 214
Configuring High Availability 214
Manually Controlling High Availability 215
Backing up an HA configuration 216
Upgrading Software in an HA Configuration 216
Using HA with Signature-based Security Services 216
Using HA with Proxy Sessions 217
CHAPTER 19 Configuring spamBlocker 219
About spamBlocker 219
spamBlocker actions 219
spamBlocker tags 219
spamBlocker categories 220
Installing the Software License 220
Activating spamBlocker 221
Configuring spamBlocker 222
Adding spamBlocker exceptions 223
Creating Rules for Bulk and Suspect E-mail on E-mail Clients 224
Sending spam or bulk e-mail to special folders in Outlook 224
Reporting False Positives and False Negatives 225
Monitoring spamBlocker Activity 225
Customizing spamBlocker using Multiple Proxies 225
APPENDIX A Types of Policies 227
Packet Filter Policies 227
Any 227
AOL 228
archie 228

auth 228
BGP 228
Citrix 228
Clarent-gateway 229
Clarent-command 229
CU-SeeMe 230
DHCP-Server or DHCP-Client 230
DNS 230
Entrust 230
finger 231
FTP 231
Gopher 231
GRE 231
HTTP 232
HTTPS 232
HBCI 232
IDENT 232
IGMP 233
IKE 233
IMAP 233
IPSec 233
IRC 234
Intel Video Phone 234
Kerberos v 4 and Kerberos v 5 234
L2TP 234
LDAP 234
LDAP-SSL 235
Lotus Notes 235
MSSQL-Monitor 235
MSSQL-Server 235
MS Win Media 235
NetMeeting 236
NFS 236
NNTP 236
NTP 236
OSPF 237
pcAnywhere 237
ping 237
POP2 and POP3 237
PPTP 238
RADIUS and RADIUS-RFC 238
RADIUS-Accounting and RADIUS-ACCT-RFC 238
RDP 238
RIP 239
RSH 239
RealPlayer G2 239
Rlogin 239

SecurID 240
SMB (Windows Networking) 240
SMTP 240
SNMP 240
SNMP-Trap 241
*SQL*Net* 241
SQL-Server 241
ssh 241
Sun RPC 241
syslog 242
TACACS 242
TACACS+ 242
TCP 242
TCP-UDP 243
UDP 243
telnet 243
Timbuktu 243
Time 243
traceroute 244
UUCP 244
WAIS 244
WinFrame 244
WG-Auth 245
WG-Firebox-Mgmt 245
WG-Logging 245
WG-Mgmt-Server 245
WG-SmallOffice-Mgmt 246
WG-WebBlocker 246
whois 246
X11 246
Yahoo Messenger 246
Proxied Policies 247
DNS 247
FTP 247
HTTP 247
SMTP 247
TCP Proxy 248

CHAPTER 1

Introduction

WatchGuard® Fireware™ Pro is the next generation of security appliance software available from WatchGuard. Appliance software is a software application that is kept in the memory of your firewall hardware. The Firebox uses the appliance software with a configuration file to operate.

Your organization's security policy is a set of rules that define how you protect your computer network and the information that passes through it. Fireware Pro appliance software has advanced features to manage security policies for the most complex networks.

Fireware Features and Tools

WatchGuard® Fireware™ Pro includes many features to improve your network security.

Policy Manager for Fireware

Policy Manager gives you one user interface for basic firewall configuration tasks. Policy Manager includes a full set of preconfigured packet filters and proxies. For example, to apply a packet filter for all Telnet traffic, you add a Telnet packet filter. You can also make a custom packet filter for which you set the ports, protocols, and other parameters. Careful configuration of IPS options can stop attacks such as SYN Flood attacks, spoofing attacks, and port or address space probes.

Firebox System Manager

Firebox® System Manager gives you one interface to monitor all components of your Firebox. From Firebox System Manager, you can monitor the current condition of the Firebox or connect directly to get an update on its configuration.

Network Address Translation

Network address translation (NAT) is a term used for one or more methods of IP address and port translation. Network administrators frequently use NAT to increase the number of computers that can operate with only one public IP address. NAT also hides the private IP addresses of computers on your network.

Firebox and third-party authentication servers

WatchGuard® System Manager with Fireware supports five different authentication servers: Firebox, RADIUS, SecurID, LDAP, and Active Directory.

Signature-based intrusion detection and prevention

When a new intrusion attack is identified, the qualities that make the virus or attack unique are identified and recorded. A unique set of qualities for a given virus or attack is known as the signature. WatchGuard Gateway AntiVirus and Intrusion Prevention Service use these signatures to find viruses and detect intrusion attacks. The Intrusion Prevention Service operates with all WatchGuard proxies. Gateway AntiVirus operates with the SMTP Proxy.

VPN creation and management

Fireware technology makes it easier to configure, manage, and monitor many IPSec VPN tunnels to branch offices and end users.

Advanced networking features

Fireware lets you configure a maximum of four Firebox interfaces as external, or WAN, interfaces. You can control the flow of traffic through more than one WAN interface to share the volume of outgoing traffic. The QoS feature in Fireware lets you set priority and bandwidth restrictions for each policy. The Firebox can also use the dynamic route protocols RIP, OSPF, and BGP. These protocols can decrease network maintenance and supply route redundancy.

Web traffic control

The WebBlocker feature uses the HTTP Proxy to apply a filter to Web traffic. You can set the hours in the day that users can get access to different types of web content. You can also set categories of web sites that users cannot browse to.

High availability

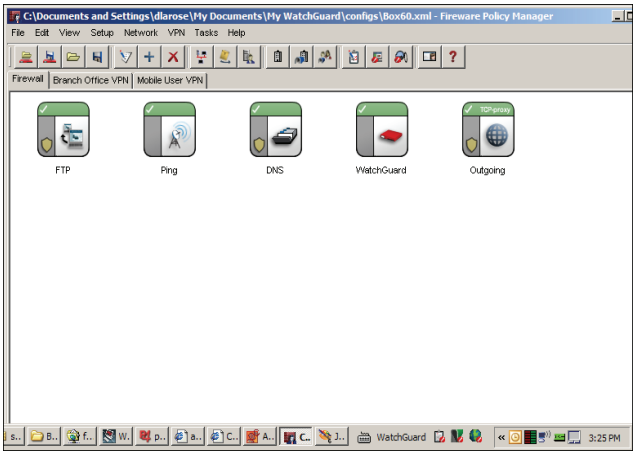
High Availability supplies stateful failover for firewall connections. With High Availability, you can have one Firebox in operation in standby mode, while the other Firebox continues to operate. The standby Firebox automatically takes over firewall operations if the primary Firebox is not able to connect with the Internet.

Fireware User Interface

The primary components of the Fireware™ user interface are Policy Manager and Firebox® System Manager.

Policy Manager window

Policy Manager includes menus you use to manage your Firebox and build your configuration file. The major menus and their options are shown below.



File menu

- Create a new configuration file
- Open a configuration file
- Save a configuration file to hard disk or to the Firebox
- Back up a Firebox
- Restore a Firebox
- Update the Firebox appliance software
- Change passphrases

Edit menu

- Change, add, and delete policies

Setup menu

- Give the Firebox model, name, location, contact, and time zone
- See, add, and download licenses
- Add, edit, or remove aliases
- Set up Log Servers
- Use internal and third-party authentication servers
- Create actions: a procedure to use when a data stream matches an applicable specification
- Configure intrusion detection and prevention settings
- Blocked sites and blocked ports settings
- Update signatures and engine settings for signature-based intrusion prevention
- Enable Network Time Protocol and add NTP servers
- Enable SNMP traps and add SNMP management stations
- Configure global settings for the Firebox

Network menu

- Configure Firebox interfaces
- Configure dynamic NAT and 1-to-1 NAT
- See and add routes
- Configure dynamic routing with the RIP, OSPF, and BGP protocols
- Configure High Availability

VPN menu

- See and add gateways
- See and configure tunnels; change authentication, encryption, and advanced IPSec settings
- Add remote users for PPTP or MUVPN
- Enable the Firebox as a managed client

Tasks menu

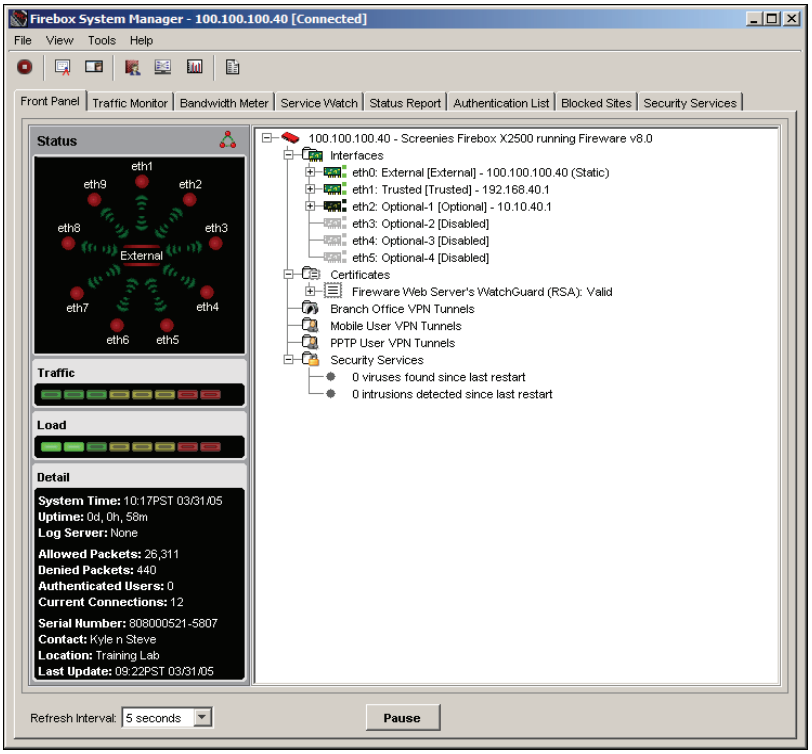
- Start wizards to activate and create a basic configuration for spamBlocker, Gateway AntiVirus, Intrusion Prevention, and WebBlocker
- Edit the configuration for spamBlocker, Gateway AntiVirus, Intrusion Prevention, and WebBlocker

Firebox System Manager window

You use Firebox System Manager to see:

- Status of the Firebox interfaces and the traffic that goes through the interfaces
- Status of VPN tunnels and management certificates
- Real-time graphs of Firebox bandwidth use or of the connections on specified ports

- Status of any security services subscriptions you use on your Firebox


Firebox System Manager - 100.100.100.40 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
Status
eth1 eth2 eth3 eth4 eth5 eth6 eth7 eth8 eth9 External
Traffic
Load
Detail
System Time: 10:17PST 03/31/05
Uptime: 0d, 0h, 58m
Log Server: None
Allowed Packets: 26,311
Denied Packets: 440
Authenticated Users: 0
Current Connections: 12
Serial Number: 808000521-5807
Contact: Kyle n Steve
Location: Training Lab
Last Update: 09:22PST 03/31/05
100.100.100.40 - Screenies Firebox X2500 running Fireware v8.0
Interfaces
eth0: External [External] - 100.100.100.40 (Static)
eth1: Trusted [Trusted] - 192.168.40.1
eth2: Optional-1 [Optional] - 10.10.40.1
eth3: Optional-2 [Disabled]
eth4: Optional-3 [Disabled]
eth5: Optional-4 [Disabled]
Certificates
Fireware Web Server's WatchGuard (RSA): Valid
Branch Office VPN Tunnels
Mobile User VPN Tunnels
PPTP User VPN Tunnels
Security Services
0 viruses found since last restart
0 intrusions detected since last restart
Refresh Interval: 5 seconds
Pause

View menu

- See the certificates on the Firebox
- See the license on the Firebox
- Open the communication log file

Tools menu

- Open Policy Manager with the configuration of the Firebox
- Open HostWatch and connect to the Firebox
- Monitor the performance aspects of the Firebox
- Synchronize the time of the Firebox with the system time
- Clear the ARP cache of the Firebox
- Clear the alarms on the Firebox
- Configure High Availability options
- Change the status and configuration passphrases

CHAPTER 2

Monitoring Firebox Status

WatchGuard® Firebox® System Manager (FSM) gives you one interface to monitor all components of a Firebox and the work it does. From FSM, you can monitor the current condition of the Firebox, or connect to the Firebox directly to update its configuration. You can see:

- Status of the Firebox interfaces and the traffic that goes through the interfaces
- Status of VPN tunnels and management certificates
- Real-time graphs of Firebox bandwidth use or of the connections on specified ports
- Status of any other security services you use on your Firebox

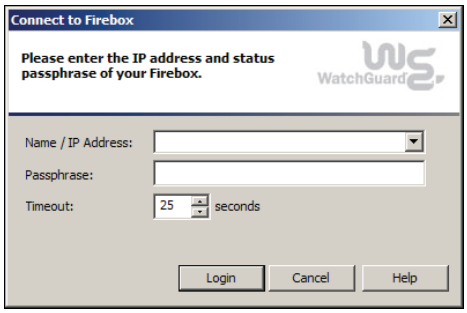
Starting Firebox System Manager

Before you start to use Firebox® System Manager, you must add a Firebox to WatchGuard® System Manager.

Connecting to a Firebox

1 From WatchGuard System Manager, click the **Connect to Device** icon.

Or, you can select **File** > **Connect To Device**.
The Connect to Firebox dialog box appears.



2 From the **Name/IP Address** drop-down list, select a Firebox.
You can also type the IP address or name of the Firebox.

3 In the **Passphrase** box, type the Firebox status (read-only) passphrase.

4 Click **Login**.
The Firebox appears in the WatchGuard System Manager window.

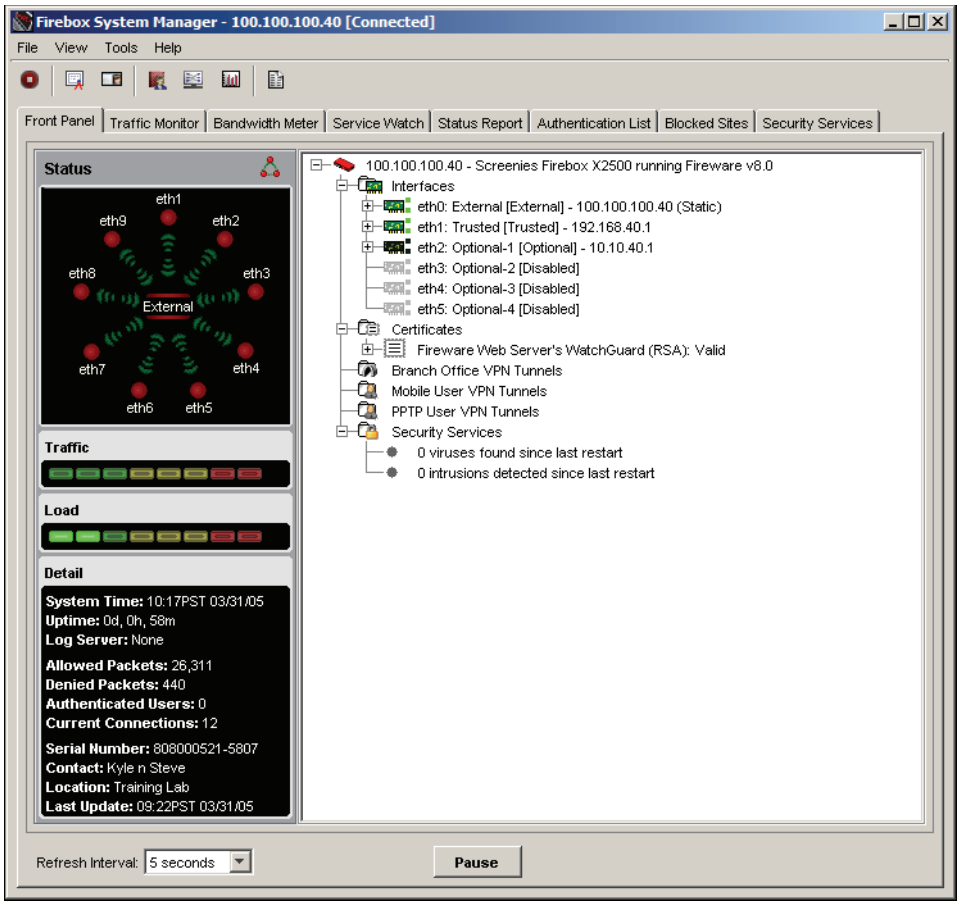
Opening Firebox System Manager

1 From WatchGuard System Manager, select the **Device Status** tab.

2 Select the Firebox to examine with Firebox System Manager.

3 Click the **Firebox System Manager** icon.

Firebox System Manager appears. Then it connects to the Firebox to get information about the status and configuration.



Firebox System Manager Menus and Toolbar

Firebox® System Manager (FSM) commands are in the menus at the top of the window. The most common tasks are also available as buttons on the toolbar. The tables that follow tell you the function of the menus and toolbar buttons.

Firebox System Manager Menus

Menu	Command	Function
File	Settings	Changes how Firebox System Manager shows status information in the displays.
	Reset	Resets Firebox System Manager statistics.
	Reboot	Starts the current Firebox again.
	Shutdown	Stops the Firebox.
	Close	Closes the Firebox System Manager window.
View	Certificates	Lists the certificates on the Firebox.
	Licenses	Lists the current licenses on the Firebox.
	Communication Log	Opens the communication log.
Tools	Policy Manager	Opens Policy Manager with the configuration of the current Firebox.
	HostWatch	Opens HostWatch connected to current Firebox.
	Performance Console	Shows graphs of performance aspects of the Firebox.
	Synchronize Time	Synchronizes the time of the Firebox with the system time.
	Clear ARP Cache	Empties the ARP cache of the current Firebox.
	Clear Alarm	Empties the alarm list on the current Firebox
	High Availability	Configures High Availability options.
	Change Passphrases	Changes the status and configuration passphrases.
Help	Firebox System Manager Help	Opens the online help files for this application.
	About	Shows version and copyright information.

Firebox System Manager Toolbar

Icon	Function
	Starts the display again. This icon appears only when you are not connected to a Firebox.
	Stops the display. This icon appears only when you are connected to a Firebox.
	Shows the management and VPN certificates saved on the Firebox.
	Shows the licenses registered and installed for this Firebox.
	Starts Policy Manager. Use Policy Manager to make or change a configuration file.
	Starts HostWatch, which shows connections for this Firebox.
	Starts the Performance Console where you can configure graphs that show Firebox status.
	Starts the Communication Log dialog box to show connections between Firebox System Manager and the Firebox.

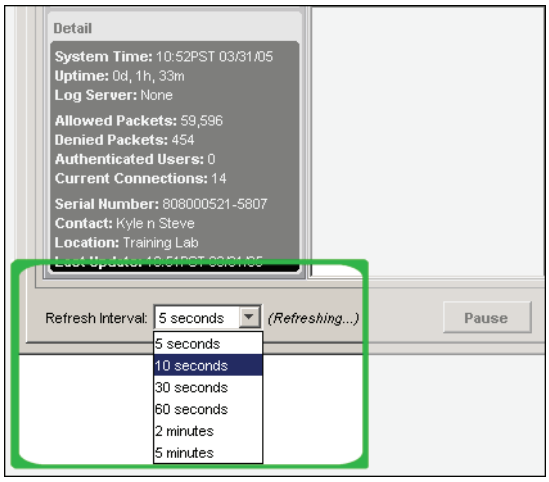
Setting refresh interval and pausing the display

All tabs on Firebox System Manager have, at the bottom of the screen, a drop-down list to set the refresh interval, and a **Pause** button to stop the display:

Refresh Interval

The refresh interval is the time between refreshes. You can change the interval of time (in seconds) that Firebox System Manager gets the Firebox information and sends updates to the user interface.

You must balance how frequently you get information and the load on the Firebox. Be sure to examine the refresh interval on each tab. When a tab gets new information for its display, the text "Refreshing..." appears adjacent to the **Refresh Interval** drop-down list. A shorter time interval gives a more accurate display, but makes more load on the Firebox. From Firebox System Manager, use the **Refresh Interval** drop-down list to select a new interval. Select the duration between window refreshes for the Bandwidth Meter. You can select 5 seconds, 10 seconds, 30 seconds, 60 seconds, 2 minutes, or 5 minutes. You can also type a custom value into this box.



Pause/Continue

You can click the **Pause** button to temporarily stop Firebox System Manager from refreshing this window. After you click the **Pause** button, this button changes to a **Continue** button. Click **Continue** to continue to refresh the window.

Seeing Basic Firebox and Network Status

The **Front Panel** tab of Firebox® System Manager shows basic information about your Firebox, your network, and network traffic.

Using the Security Traffic Display

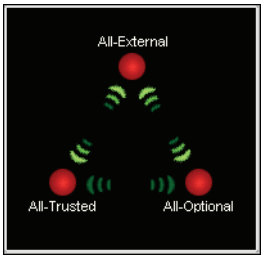
Firebox System Manager initially has a group of indicator lights to show the direction and volume of the traffic between the Firebox interfaces. The display can be a triangle (below left) or a star (below center and right).

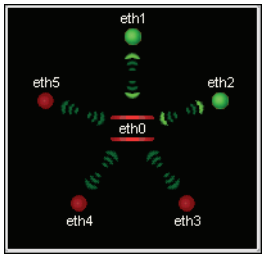
Triangle display

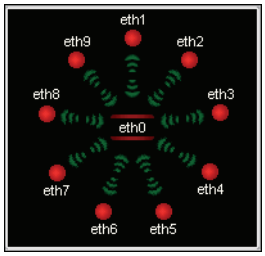
If a Firebox has only three configured interfaces, each corner of the triangle is one interface. If a Firebox has more than three interfaces, each corner of the triangle represents one type of interface. For example, if you have six configured interfaces with one external, one trusted, and four optional interfaces, the "All-Optional" corner in the triangle represents all four of the optional interfaces.

Star display

The star display shows all traffic in and out of the center interface. An arrow that moves from the center interface to a node interface shows that the Firebox is passing traffic. The traffic comes in through the center interface and goes out through the node interface. For example, if eth1 is at the center and eth2 is at a node, a green arrow shows that traffic flows from eth1 to eth2. There are two star displays — one for a Firebox X Core with 6 interfaces and one for Firebox X Peak with 10 interfaces.







To change the display, right-click it and select **Triangle Mode** or **Star Mode**.

Monitoring status information

The points of the star and triangle show the traffic that flows through the interfaces. Each point shows incoming connections and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows come on in the direction of the traffic.

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny)—The Firebox denies a connection on that interface.
- Green (allow)—There is traffic between this interface and a different interface (but not the center) of the star. When there is traffic between this interface and the center, the point between these interfaces shows as green arrows.

In the triangle, the network traffic shows in the points of the triangle. The points show only the idle or deny condition. One exception is when there is a large quantity of VPN tunnel switching traffic. "Tunnel switching" traffic refers to packets that are sent through a VPN to a Firebox configured as the default gateway for the VPN network. In this case, the Firebox System Manager traffic level indicator can show very high traffic, but you do not see green lights as move tunnel switching traffic comes in and goes out of the same interface.

Setting the center interface

If you use the star figure, you can customize the interface that appears in its center. Click the interface name or its point. The interface then moves to the center of the star. All the other interfaces move clockwise. If you move an interface to the center of the star, you can see all traffic between that interface and all other interfaces. The default display shows the external interface in the center.

Monitoring traffic, load, and status

Below the **Security Traffic Display** are the traffic volume indicator, processor load indicator, and basic status information (Detail).

The two bar graphs show the traffic volume and the Firebox capacity.

Firebox and VPN tunnel status

The section in Firebox System Manager to the right side of the front panel shows:

- The status of the Firebox
- The branch office VPN tunnels
- The mobile user and PPTP VPN tunnels
- Viruses, intrusions, and spam e-mail messages found

Firebox Status

In the Firebox Status section, you see:

- Status of the High Availability feature. When it has a correct configuration and is available, the IP address of the standby Firebox appears. If High Availability is installed, but there is no network connection to the secondary Firebox, a "Not Responding" message appears.
- The IP address of each Firebox interface and the configuration mode of the external interface.
- Status of the CA (root) certificate and the IPSec (client) certificate.

If you expand the entries in the Firebox System Manager main window, you can see:

- IP address and netmask of each configured interface
- The Media Access Control (MAC) address of each interface
- Number of packets that are sent and received since the last Firebox restart
- End date and time of CA and IPSec certificates
- CA fingerprint. Use this to find man-in-the-middle attacks
- Status of the physical link (a dark icon indicates the connection is down)

Branch Office VPN Tunnels

Below the Firebox Status section is a section on BOVPN tunnels. There are two types of IPSec BOVPN tunnels: tunnels you create manually and tunnels you create with the Management Server.

Note

Because Fireware supports only a single routing policy per tunnel, only one policy appears, even if you configure more than one.

Mobile User VPN Tunnels

When the branch office VPN tunnels are entries for Mobile User VPN tunnels, the entry shows similar information as for Branch Office VPN.

PPTP User VPN Tunnels

For PPTP User VPN tunnels, Firebox System Manager shows the quantity of sent and received packets.

Security Services

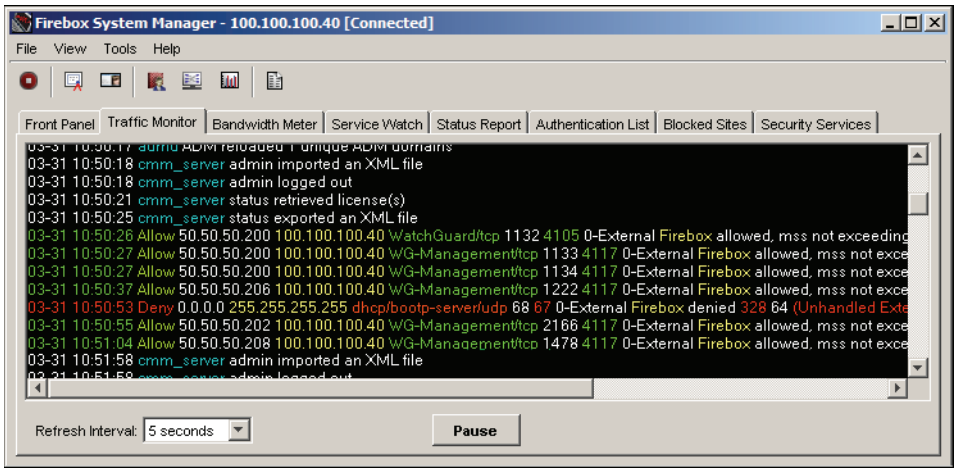
Below Security Services, Firebox System Manager includes the number of viruses found, the number of intrusions, and the number of spam e-mail messages that are blocked and effectively quarantined since the last restart.

Expanding and closing tree views

To expand a part of the display, click the plus sign (+) adjacent to the entry, or double-click the name of the entry. To close a part, click the minus sign (–) adjacent to the entry. When no plus or minus sign shows, no more information is available.

Monitoring Firebox Traffic

To see Firebox® log messages, click the **Traffic Monitor** tab.

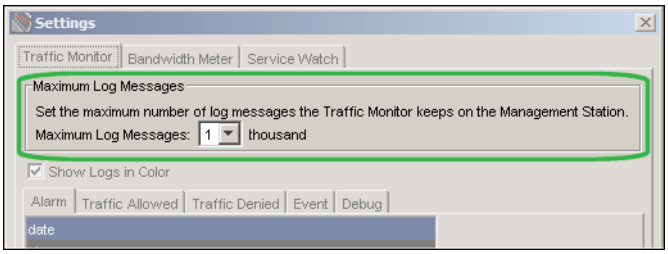

Firebox System Manager - 100.100.100.40 [Connected]
File View Tools Help
Front Panel
Traffic Monitor
Bandwidth Meter
Service Watch
Status Report
Authentication List
Blocked Sites
Security Services
03-31 10:50:18 cmm_server admin imported an XML file
03-31 10:50:18 cmm_server admin logged out
03-31 10:50:21 cmm_server status retrieved license(s)
03-31 10:50:25 cmm_server status exported an XML file
03-31 10:50:26 Allow 50.50.50.200 100.100.100.40 WatchGuard/tcp 1132 4105 0-External Firebox allowed, mss not exceeding
03-31 10:50:27 Allow 50.50.50.200 100.100.100.40 WG-Management/tcp 1133 4117 0-External Firebox allowed, mss not exce
03-31 10:50:27 Allow 50.50.50.200 100.100.100.40 WG-Management/tcp 1134 4117 0-External Firebox allowed, mss not exce
03-31 10:50:37 Allow 50.50.50.206 100.100.100.40 WG-Management/tcp 1222 4117 0-External Firebox allowed, mss not exce
03-31 10:50:53 Deny 0.0.0.0 255.255.255.255 dhcp/bootp-server/udp 68 67 0-External Firebox denied 328 64 (Unhandled Exte
03-31 10:50:55 Allow 50.50.50.202 100.100.100.40 WG-Management/tcp 2166 4117 0-External Firebox allowed, mss not exce
03-31 10:51:04 Allow 50.50.50.208 100.100.100.40 WG-Management/tcp 1478 4117 0-External Firebox allowed, mss not exce
03-31 10:51:58 cmm_server admin imported an XML file
Refresh Interval: 5 seconds
Pause

Setting the maximum number of log messages

You can change the maximum number of log messages that you can keep and see on Traffic Monitor. When you get to the maximum number, the new log messages replace the first entries. If you have a

slow processor or a small quantity of RAM, a high value in this field can slow your management system. If it is necessary to examine a large volume of log messages, we recommend that you use Log Viewer.

1 From Firebox System Manager, select **File > Settings**.
The Settings dialog box appears.

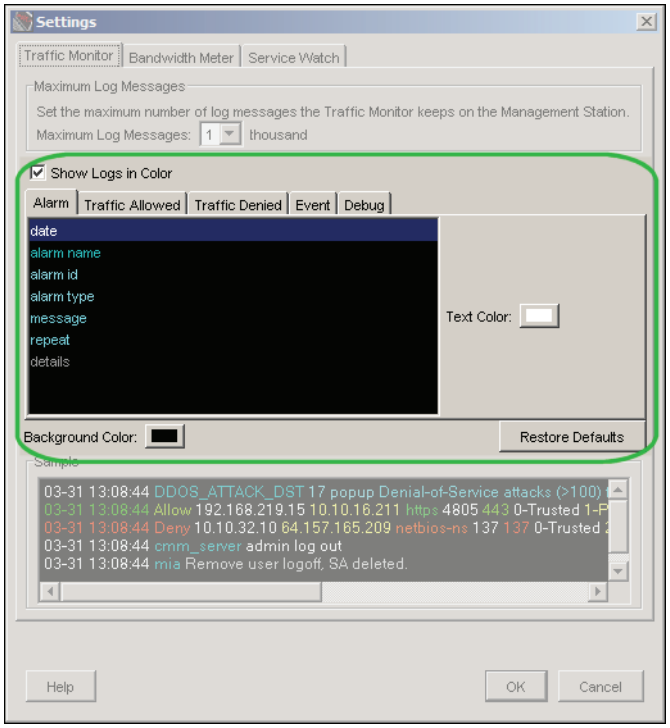


2 From the **Maximum Log Messages** drop-down list, select the number of log messages that you want to appear in Traffic Monitor. Click **OK**.
The value you type gives the number of log messages in thousands.

Using color for your log messages

In Traffic Monitor, you can make log messages appear in different colors. Each color can refer to the types of information they show.

1 From Firebox System Manager, select **File > Settings**. Click the **Traffic Monitor** tab.



2 To enable the display of colors, select the **Show Logs in Color** check box.

3 On the **Alarm**, **Traffic Allowed, Traffic Denied**, **Event**, or **Debug** tab, click the field to appear in a color.
The Text Color field on the right side of the tabs shows the color in use for the field.

4 To change the color, click the color control adjacent to **Text Color.** Select a color. Click **OK** to close the color control dialog box. Click **OK** again to close the **Settings** dialog box.
The information in this field appears in the new color on Traffic Monitor. A sample of how Traffic Monitor looks appears at the bottom of the dialog box.

5 You can also select a background color for the traffic monitor. Click the color control arrow adjacent to **Background Color**. Select a color. Click **OK** to close the color control dialog box. Click **OK** again to close the **Settings** dialog box.

You can cancel the changes you make in this dialog box. Click **Restore Defaults**.

Copying log messages

To make a copy of a log message and paste it in a different tool, right-click the message and select **Copy Selection.** If you select **Copy All**, Firebox System Manager copies all the log messages. Open the other tool and paste the message or messages.

To copy more than one, but not all, log messages, use Log Viewer to open the log file, and then use the Log Viewer copy function, as described in the *WatchGuard® System Manager User Guide*.

Learning more about a traffic log message

To learn more about a traffic log message, you can:

Copy the IP address of the source or destination

Make a copy of the source or destination IP address of a traffic log message, and paste it into a different software application. To copy the source IP address, right-click the message, and select **Source IP Address > Copy Source IP Address**. To copy the destination IP address, right-click the message, and select **Destination IP Address > Copy Destination IP Address**.

Ping the source or destination

To ping the source or destination IP address of a traffic log message, do this: Right-click the message, and select **Source IP Address > Ping** or **Destination IP Address > Ping**. A pop-up window shows the results.

Trace the route to the source or destination

To use a traceroute command to the source or destination IP address of a traffic log message, do this: Right-click the message, and select **Source IP Address** > **Trace Route** or **Destination IP Address** > **Trace Route**. A pop-up window shows you the results of the traceroute.

Temporarily block the IP address of the source or destination

To temporarily block all traffic from a source or destination IP address of a traffic log message, do this: Right-click the message, select **Source IP Address > Block: [***IP address***]** or **Destination IP Address > Block: [***IP address***]**. The length of the time that an IP address is temporarily blocked by this command is set in Policy Manager. To use this command you must give the configuration password.

Clearing the ARP Cache

The ARP (Address Resolution Protocol) cache on the Firebox® keeps the hardware addresses (also known as MAC addresses) of TCP/IP hosts. Before an ARP request starts, the system makes sure that a hardware

address is in the cache. You must clear the ARP cache on the Firebox when your network has a drop-in configuration.

1 From Firebox System Manager, select **Tools > Clear ARP Cache**.

2 Type the Firebox configuration passphrase. Click **OK**.
This flushes the cache entries.

When a Firebox is in drop-in mode, this procedure clears only the content of the ARP table and not the MAC table. The oldest MAC entries in the MAC table are removed if the table has more than 2000 entries. If you want to clear the MAC table, you must restart the Firebox.

Using the Performance Console

The Performance Console is a Firebox® utility that you use to prepare graphs that show how different parts of the Firebox are operating. To get the information, you define the counters that identify the information that is used to make the graph.

Types of counters

You can monitor these types of performance counters:

System Information
Show how the CPU is used.

Interfaces
Monitor and report on the events of selected interfaces. For example, you can set up a counter that monitors the number of packets a specified interface receives.

Policies
Monitor and report on the events of selected policies. For example, you can set up a counter that monitors the number of packets that a specified policy examines.

VPN Peers
Monitor and report on the events of selected VPN policies.

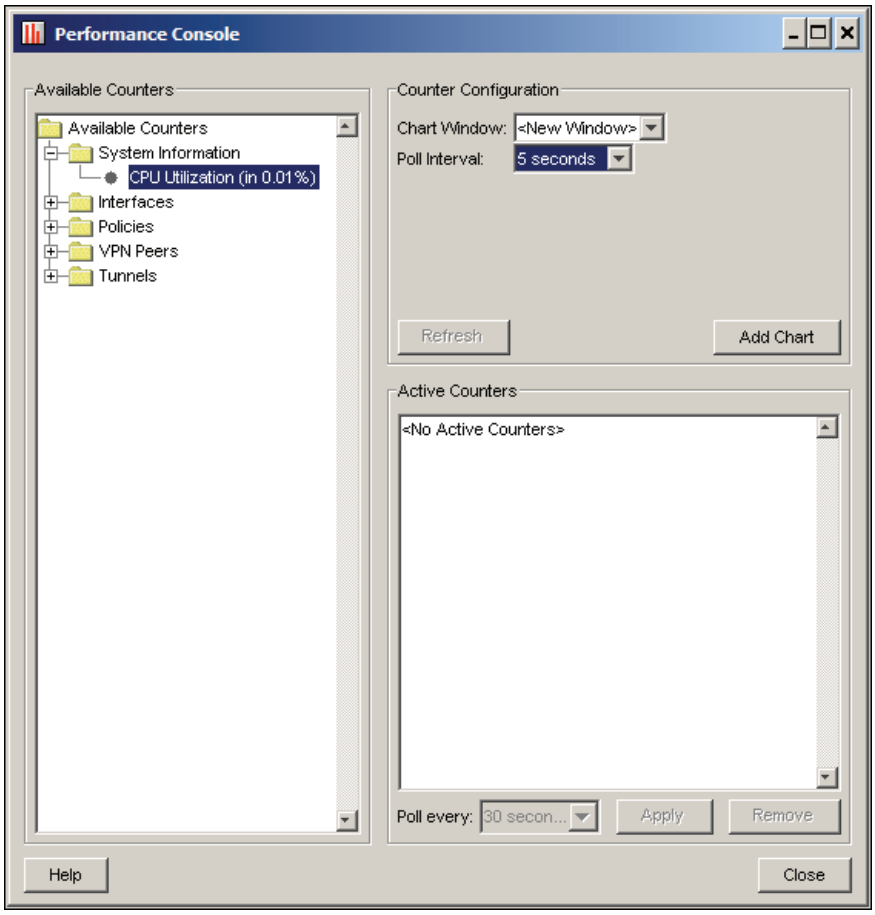
Tunnels
Monitor and report on the events of selected VPN tunnels.

Defining counters

To identify a counter for any of the categories:

1 From Firebox System Manager, select the Performance Console icon. Or, select **Tools > Performance Console**.
The Performance Console window appears.

1 From the **Performance Console** window, expand one of the counter categories that appears below **Available Counters**.
Click the + sign adjacent to the category name to see the counters you can use in that category. When you click a counter, the Counter Configuration fields automatically refresh, related to the counter you select.



2 From the **Chart Window** drop-down list, select **New Window** if the graph appears in a new window. Or, select the name of an open window to add the graph to a window that is open.

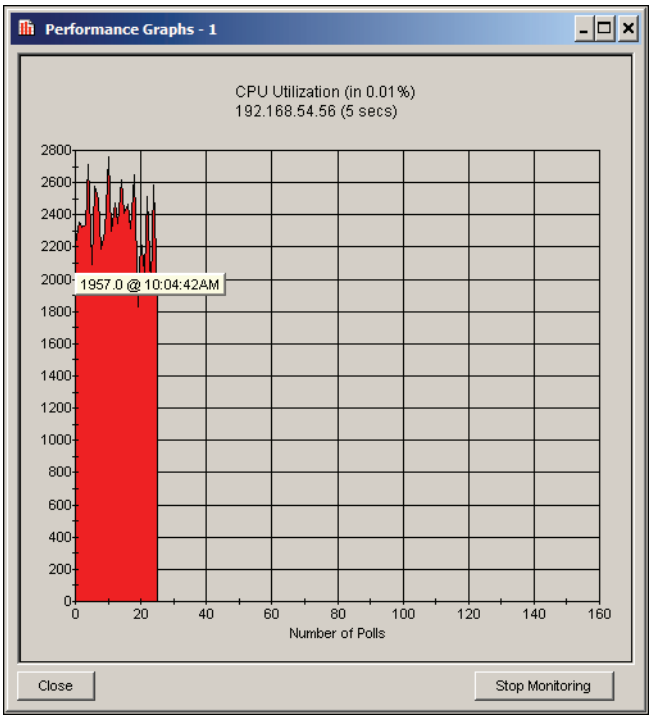
3 From the **Poll Interval** drop-down list, select a time interval between 5 and 60 seconds.
This is the frequency that the Performance Console checks for updated information from the Firebox.

4 Add configuration information that applies to the specified counter. These fields show automatically when you select specified counters.

- **Type** — Use the drop-down list to select the type of graph to create.
- **Interface** — Use the drop-down list to select the interface to graph data for.
- **Policy** — Use the drop-down list to select a policy from your Firebox configuration to graph data for.
- **Peer IP** — Use the drop-down list to select the IP address of a VPN endpoint to graph data for.

- **Tunnel ID** — Use the drop-down list to select the name of a VPN tunnel to graph data for.

5 Click **Create Chart** to start a real-time graph of this counter.



Note

This performance graph shows CPU usage. You create graphs for other functions in the same way.

To edit the polling interval of an active counter:

1 Select the counter name in the **Active Counters** dialog box in the lower-right corner of the **Performance Console** window.

2 From the **Poll every** drop-down list, select a new polling interval.

3 Click **Apply**.
The real-time chart window updates with the new polling interval.

To remove an active counter:

1 Select the counter name in the **Active Counters** dialog box in the lower-right corner of the Performance Console window.

2 Click **Remove**.

Viewing the performance graph

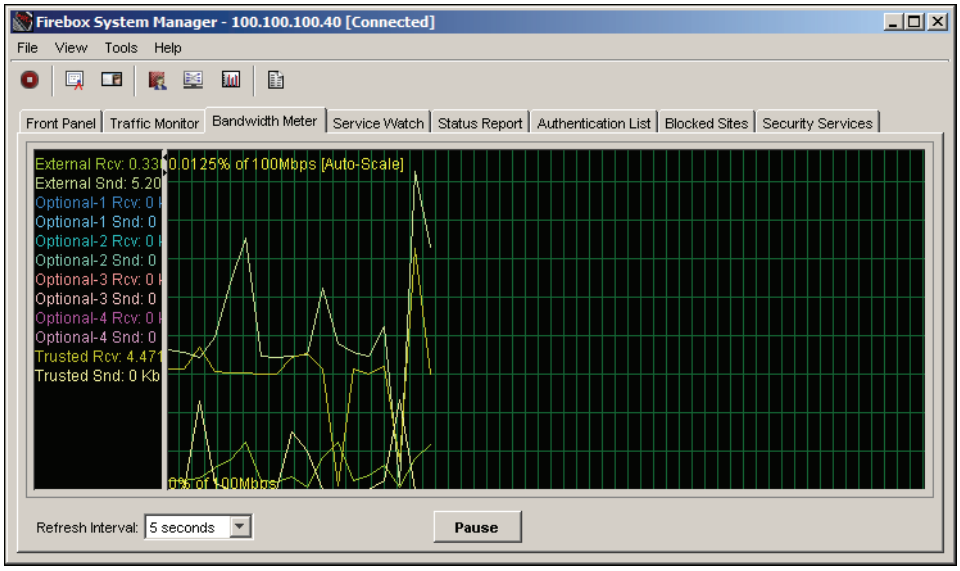
Graphs are shown in a real-time chart window. You can show one graph in each window, or show many graphs in one window. Graphs automatically scale to fit the data.

Click **Stop Monitoring** to stop the Performance Console from getting data for this counter. You can stop this monitor to save resources and restart it at different time.

Click **Close** to close the chart window. The data in the chart is not saved.

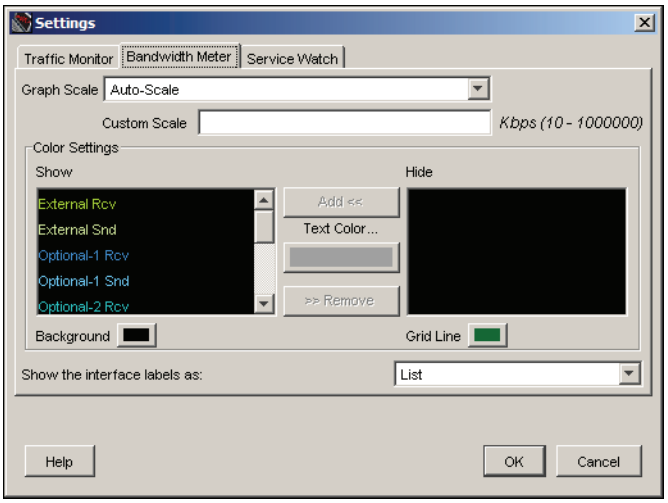
Viewing Bandwidth Usage

Select the **Bandwidth Meter** tab to see the real-time bandwidth for all the Firebox® interfaces. If you click any location on the chart, you can get more detail information in a pop-up window about bandwidth use at this point in time.



To change how the bandwidth appears:

1 From Firebox System Manager, select **File > Settings**. Click the **Bandwidth Meter** tab.



2 Do one or more of the steps in the sections below.

Changing the scale of the bandwidth display

You can change the scale of the **Bandwidth Meter** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the speed of your network. You can also set a custom scale. Type the value in kilobytes for each second in the **Custom Scale** text box.

Adding and removing lines in the bandwidth display

- To add a line to the **Bandwidth Meter** tab, select the interface from the **Hide** list in the Color Settings section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.
- To remove a line from the **Bandwidth Meter** tab, select the interface from the **Show** list in the Color Settings section. Click **Remove**. The interface name appears in the **Hide** list.

Changing colors in the bandwidth display

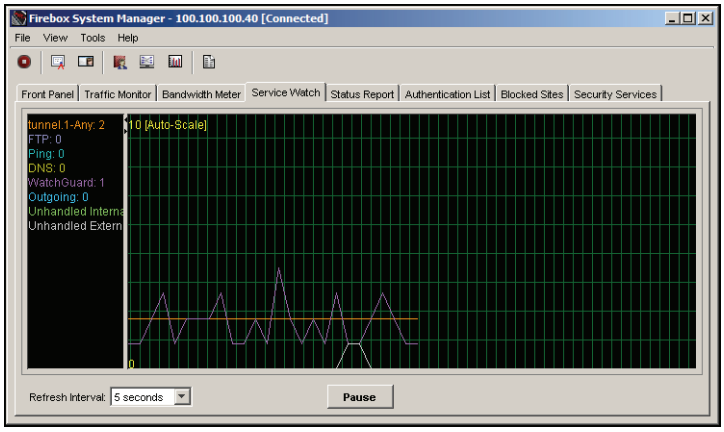
You can also change the colors of the display of the **Bandwidth Meter** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

Changing how interfaces appear in the bandwidth display

One option is to change how the interface names appear on the left side of the **Bandwidth Meter** tab. The names can show as a list. The display can also show an interface name adjacent to the line it identifies. Use the **Show the interface** text as a drop-down list to select **List** or **Tags**.

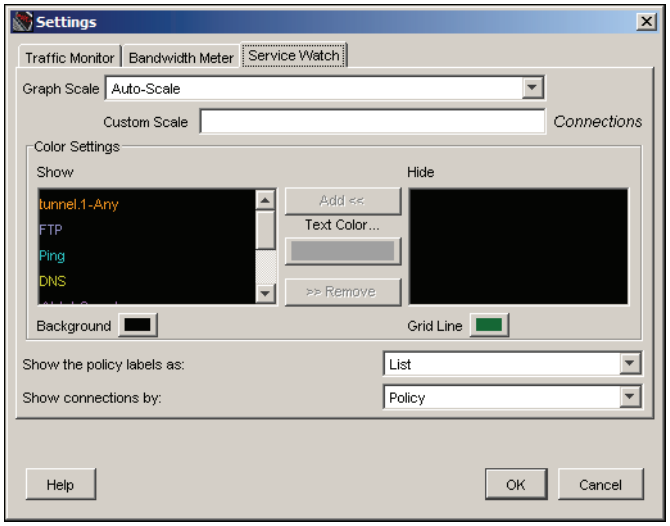
Viewing Number of Connections by Policy

Select the **Service Watch** tab of Firebox® System Manager to see a graph of the policies that are configured in Policy Manager for a Firebox. The Y axis (vertical) shows the number of connections. The X axis (horizontal) shows the time. If you click any location on the chart, you can get more detailed information in a pop-up window about policy use at this point in time.



1 To change the how the policies appear, select **File > Settings.** Click the **Service Watch** tab.

2 Do one or more of the steps in the sections below.



Changing the scale of the policies display

You can change the scale of the **Service Watch** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the volume of traffic on your network. You can also set a custom scale. Type the number of connections in the **Custom Scale** text box.

Adding and removing lines in the policies display

- To add a line to the **Service Watch** tab, select the policy from the **Hide** list in the Color Settings section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.
- To remove a line from the **Service Watch** tab, select the policy from the **Show** list in the Color Settings section. Click **Remove**. The interface name appears in the **Hide** list.

Changing colors in the policies display

You can change the colors of the display of the **Service Watch** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

Changing how policy names appear in the policies display

You can change how the policy names appear on the left side of the **Service Watch** tab. The names can show as a list. The tab can also show an interface name adjacent to the line it identifies. Use the **Show the policy labels as** drop-down list to select **List** or **Tags**.

Showing connections by policy or rule

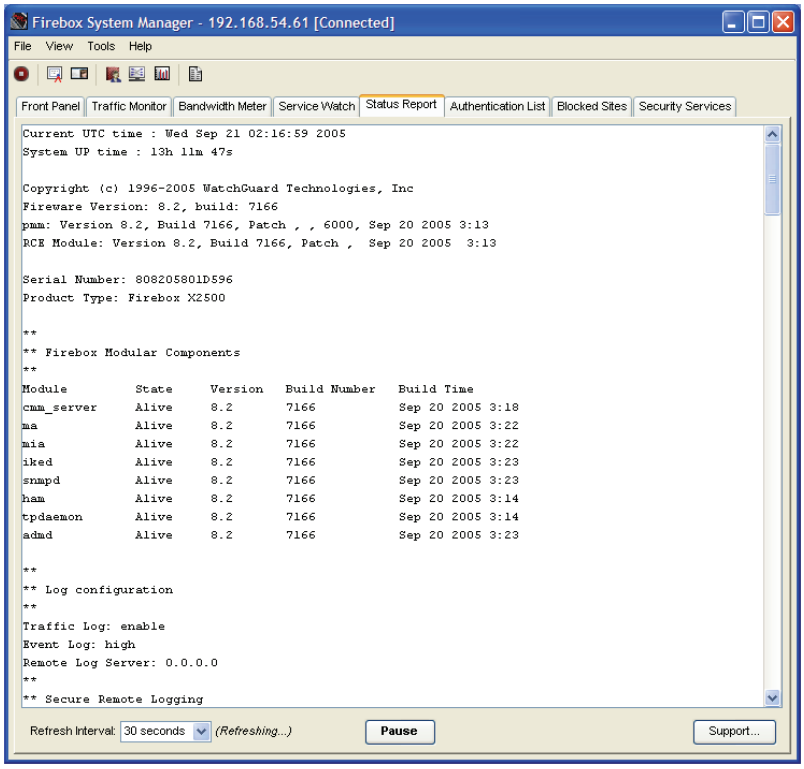
The **Service Watch** tab can show the number of connections by policy or rule. If you show by policy, then you can see more than one rule on one line. Use the **Show connections by** drop-down list to select a display setting.

Viewing Information About Firebox Status

There are four tabs that tell about Firebox® status and configuration: **Status Report**, **Authentication List**, **Blocked Sites**, and **Security Services**.

Status Report

The **Status Report** tab gives you statistics about Firebox traffic.


Firebox System Manager - 192.168.54.61 [Connected]
File View Tools Help
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites Security Services
Current UTC time : Wed Sep 21 02:16:59 2005
System UP time : 13h 11m 47s
Copyright (c) 1996-2005 WatchGuard Technologies, Inc
Fireware Version: 8.2, build: 7166
pmm: Version 8.2, Build 7166, Patch , , 6000, Sep 20 2005 3:13
RCE Module: Version 8.2, Build 7166, Patch , Sep 20 2005 3:13
Serial Number: 808205801D596
Product Type: Firebox X2500
** Firebox Modular Components
Module State Version Build Number Build Time
cmm_server Alive 8.2 7166 Sep 20 2005 3:18
ma Alive 8.2 7166 Sep 20 2005 3:22
mia Alive 8.2 7166 Sep 20 2005 3:22
iked Alive 8.2 7166 Sep 20 2005 3:23
snmpd Alive 8.2 7166 Sep 20 2005 3:23
ham Alive 8.2 7166 Sep 20 2005 3:14
tpdaemon Alive 8.2 7166 Sep 20 2005 3:14
admd Alive 8.2 7166 Sep 20 2005 3:23
** Log configuration
Traffic Log: enable
Event Log: high
Remote Log Server: 0.0.0.0
** Secure Remote Logging
Refresh Interval: 30 seconds (Refreshing...) Pause Support...

The Firebox Status Report contains this information:

Uptime and version information
: The Firebox uptime, the WatchGuard® Firebox System software version, the Firebox model, and appliance software version. There is also a list of the status and version of the product components on the Firebox.

Log hosts
: The IP addresses of the log host or hosts.

Logging options
: Log message options that are configured with the Quick Setup Wizard or Policy Manager.

Memory and load average
: Statistics on the memory use (shown in bytes of memory) and load average of the Firebox.

Processes
: The process ID, the name of the process, and the status of the process, as shown in the figure on the subsequent page. (These codes appear under the column marked “S.”)

Network configuration

Information about the network cards in the Firebox: the interface name, its hardware and software addresses, and its netmask. The display also includes local routing information and IP aliases.

Blocked Sites list

The current manually blocked sites and any current exceptions. Temporarily blocked site entries appear on the **Blocked Sites** tab.

Interfaces

Each Firebox interface appears in this section, along with information about the type of interface it is configured as (external, trusted, or optional), its status and packet count.

Routes

The Firebox kernel routing table. You use these routes to find which Firebox interface is used for each destination address.

ARP table

The ARP table on the Firebox. The ARP table is used to match IP addresses to hardware addresses. (When an appliance is in drop-in mode, use the contents of the ARP table only to troubleshoot connectivity over secondary networks on the interfaces.)

Dynamic Routing

This shows which, if any, dynamic routing components are in use on the Firebox.

Refresh interval

This is the rate at which this display updates the information.

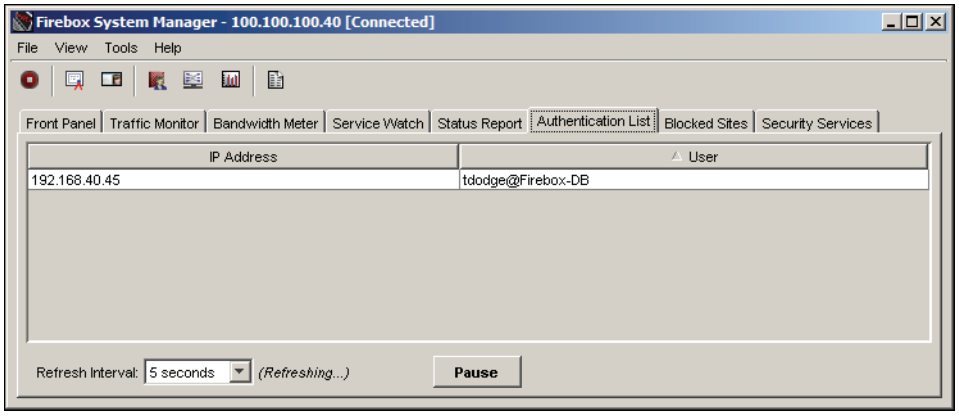
Support

Click **Support** to open the **Support Logs** dialog box. This is where you set the location to which you save the diagnostic log file. You save a support log in tarzipped (*.tgz) format. You create this file for troubleshooting, when asked by your support representative.

Authentication List

The **Authentication List** tab of Firebox System Manager gives the IP addresses and user names of all the persons that are authenticated to the Firebox. If you use DHCP, an IP address can appear as a different user name when the computer starts again.

You can click the column header to sort users by IP address. You can also remove an authenticated user from the list. To do this, right-click their user name and then stop their authenticated session.



Blocked Sites

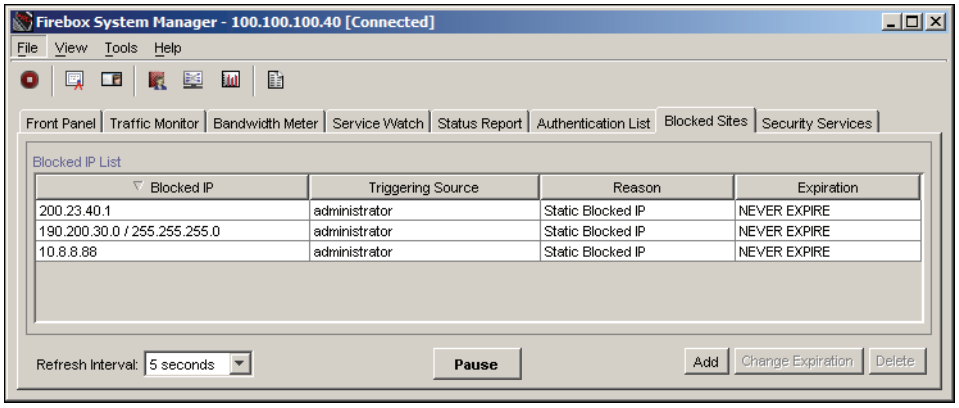
The **Blocked Sites List** tab of Firebox System Manager shows the IP addresses of all the external IP addresses that are temporarily blocked. Many events can cause the Firebox to add an IP address to the **Blocked Sites** tab: a port space probe, a spoofing attack, an address space probe, or an event you configure.

Adjacent to each IP address is the time when it comes off the **Blocked Sites** tab. You can use the **Blocked Sites** dialog box in Policy Manager to adjust the length of time that an IP address stays on the list.

Adding and removing sites

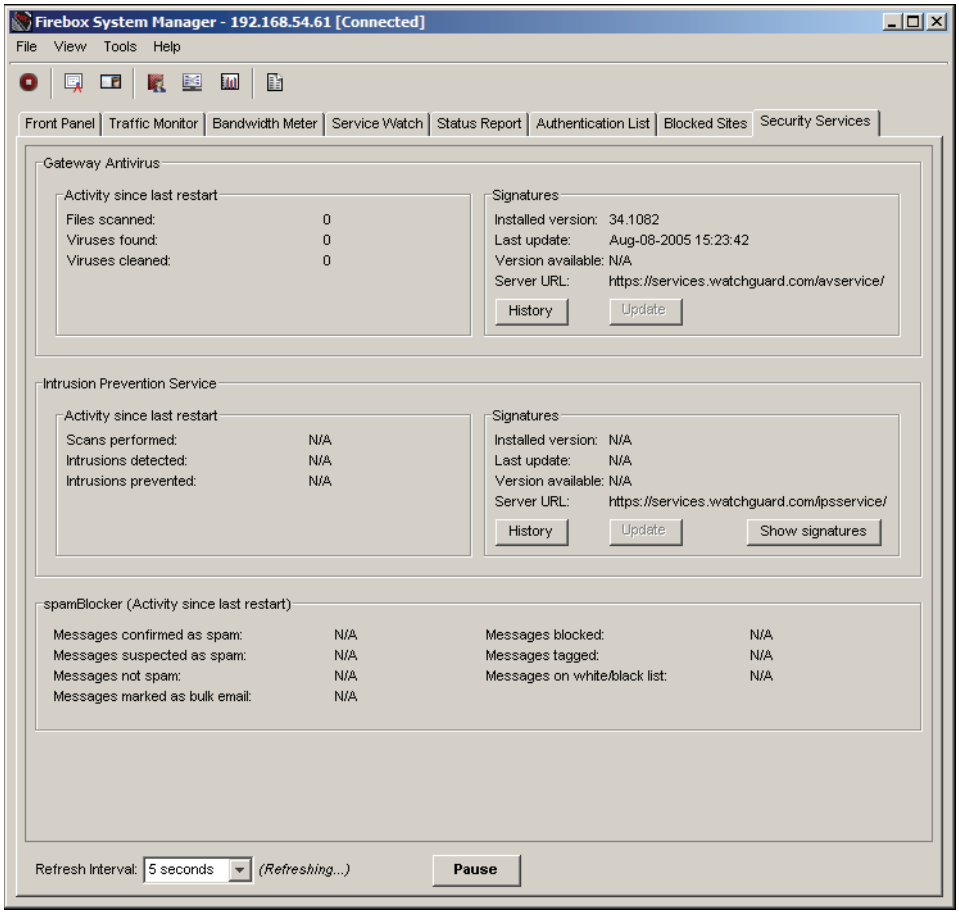
The **Blocked Sites** tab is in continuous refresh mode if the **Continue** button on the toolbar (shown at right) is enabled. **Add** allows you to temporarily add a site to the blocked sites list. Click **Change Expiration** to change the time at which this site is deleted from the list. **Delete** removes the site from the blocked sites list.

If you open the Firebox with the status passphrase, you must type the configuration passphrase before you can remove a site from the list.



Security Services

The **Security Services** tab includes information about the Gateway AntiVirus and Intrusion Prevention services.



Gateway AntiVirus

This area of the dialog box gives information about the Gateway AntiVirus feature.

Activity since last restart

- Files scanned: Number of files scanned for viruses since the last Firebox restart.
- Viruses found: Number of viruses found in scanned files since the last Firebox restart.
- Viruses cleaned: Number of infected files deleted since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates.
- Update: Click to update your virus signatures. This button is active only if a new version of the virus signatures is available.

Intrusion Prevention Service

This area of the dialog box gives information about the Signature-Based Intrusion Prevention Service feature.

Activity since last restart

- Scans performed: Number of files scanned for viruses since the last Firebox restart.
- Intrusions detected: Number of viruses found in scanned files since the last Firebox restart.
- Intrusions prevented: Number of infected files deleted since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates.
- Update: Click this button to update your intrusion prevention signatures. This button is active only if a new version of the intrusion prevention signatures is available.
- Show signatures: Click this button to download and show a list of all current IPS signatures. After you download the signatures, you can look for signatures by signature ID.

spamBlocker

Activity since last restart

- Number of messages that are identified as not spam, spam, bulk, or suspect e-mail.
- Number of messages that are blocked, tagged, and on the white/black list.

Using HostWatch

HostWatch is a graphic user interface that shows the network connections between the trusted and external networks. HostWatch also gives information about users, connections, and network address translation (NAT).

The line that connects the source host and the destination host uses a color that shows the type of connection. You can change these colors. The default colors are:

- **Red** — The Firebox® denies the connection.
- **Blue** — The connection uses a proxy.
- **Green** — The Firebox uses NAT for the connection.
- **Black —** Normal connection.

Icons that show the type of service appear adjacent to the server entries for HTTP, Telnet, SMTP, and FTP.

Domain name server (DNS) resolution does not occur immediately when you start HostWatch. When HostWatch is configured for DNS resolution, it replaces the IP addresses with the host or user names. If the Firebox cannot identify the host or user name, the IP address stays in the HostWatch window.

If you use DNS resolution with HostWatch, the management station can send a large number of NetBIOS packets (UDP 137) through the Firebox. The only method to stop this is to turn off NetBIOS over TCP/IP in Windows.

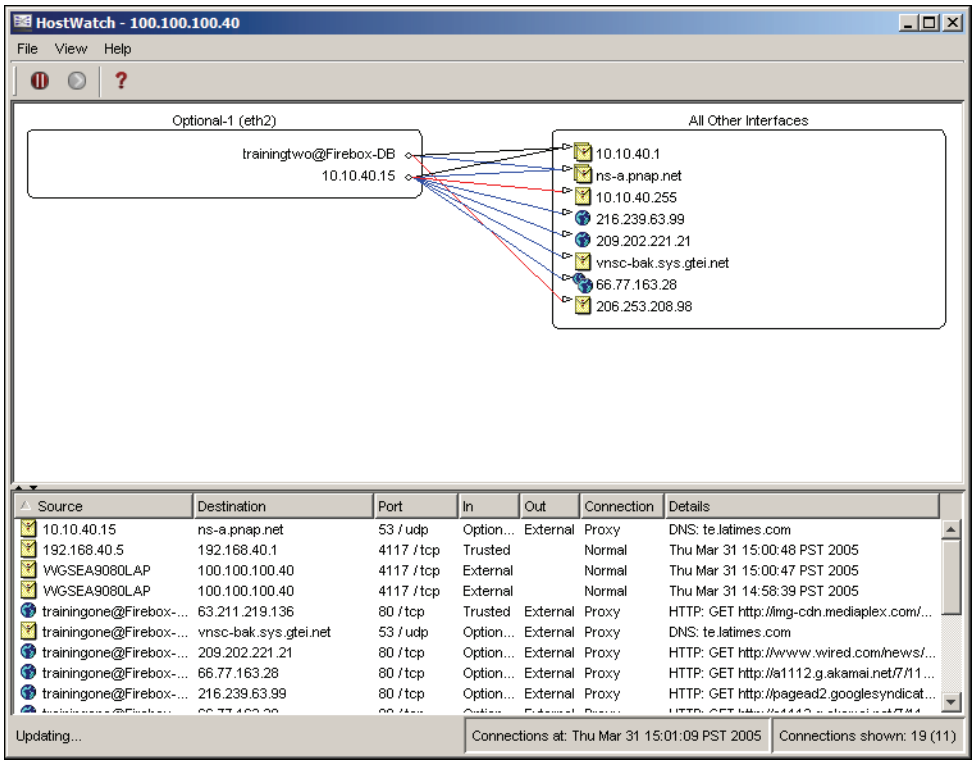
To start **HostWatch**, click the **HostWatch** icon in Firebox System Manager.
Or select **Tools > HostWatch**.

The HostWatch window

The top part of the HostWatch window has two sides. You can set the interface for the left side. The right side shows all other interfaces. HostWatch shows the connections to and from the interface configured on the left side. To select an interface, right-click the current interface name. Select the new interface.

Double-click an item on one of the sides to get the **Connections For** dialog box. The dialog box shows information about the connection, and includes the IP addresses, port number, time, connection type, and direction.

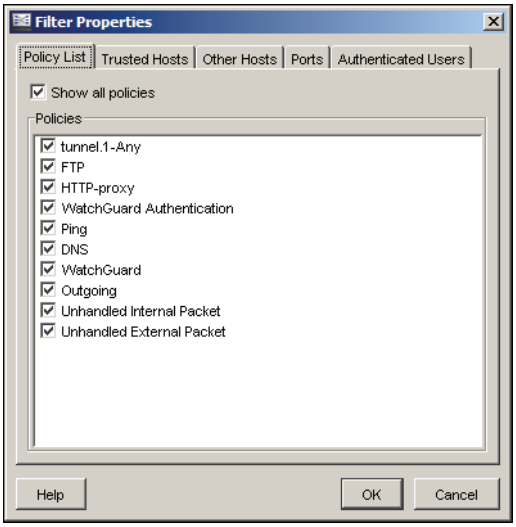
While the top part of the window only shows the connections to and from the selected interface, the bottom of the HostWatch window shows all connections to and from all interfaces. The information is shown in a table with the ports and the time the connection was created.


HostWatch - 100.100.100.40
File View Help
Optional-1 (eth2)
trainingtwo@Firebox-DB
10.10.40.15
All Other Interfaces
10.10.40.1
ns-a.pnap.net
10.10.40.255
216.239.63.99
209.202.221.21
vnsc-bak.sys.gtei.net
66.77.163.28
206.253.208.98
Source Destination Port In Out Connection Details
10.10.40.15 ns-a.pnap.net 53 / udp Option... External Proxy DNS: te.latimes.com
192.168.40.5 192.168.40.1 4117 / tcp Trusted Normal Thu Mar 31 15:00:48 PST 2005
WGSEA9080LAP 100.100.100.40 4117 / tcp External Normal Thu Mar 31 15:00:47 PST 2005
WGSEA9080LAP 100.100.100.40 4117 / tcp External Normal Thu Mar 31 14:58:39 PST 2005
trainingone@Firebox-... 63.211.219.136 80 / tcp Trusted External Proxy HTTP: GET http://img-cdn.mediaplex.com/...
trainingone@Firebox-... vnsc-bak.sys.gtei.net 53 / udp Option... External Proxy DNS: te.latimes.com
trainingone@Firebox-... 209.202.221.21 80 / tcp Option... External Proxy HTTP: GET http://www.wired.com/news/...
trainingone@Firebox-... 66.77.163.28 80 / tcp Option... External Proxy HTTP: GET http://a1112.g.akamai.net/7/11...
trainingone@Firebox-... 216.239.63.99 80 / tcp Option... External Proxy HTTP: GET http://pagead2.googlesyndicat...
Updating...
Connections at: Thu Mar 31 15:01:09 PST 2005
Connections shown: 19 (11)

Controlling the HostWatch window

You can change the HostWatch window to show only the necessary items. You can use this feature to monitor specified hosts, ports, or users.

1 From HostWatch, select **View > Filter**.



2 Click the tab to monitor: **Policy List**, **External Hosts**, **Other Hosts**, **Ports**, or **Authenticated Users**.

3 On the tab for each item you do not want to see, clear the check boxes in the dialog box.

4 On the tab for each item you do want to see, type the IP address, port number, or user name to monitor. Click **Add**. Do this for each item that HostWatch must monitor.

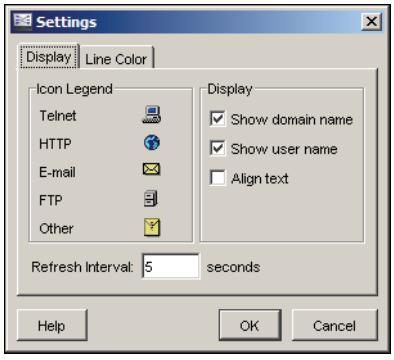
5 Click **OK**.

Changing HostWatch view properties

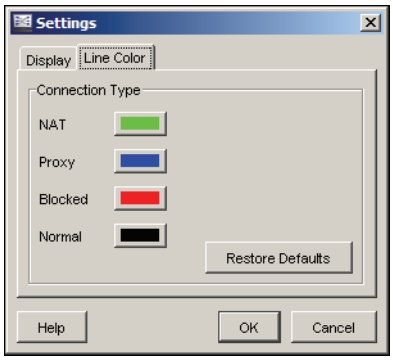
You can change how HostWatch shows information. For example, HostWatch can show host names as an alternative to addresses.

1 From HostWatch, select **View > Settings**.

2 Use the **Display** tab to change how the hosts appear in the HostWatch window.



3 Use the **Line Color** tab to change the colors of the lines between NAT, proxy, blocked, and normal connections.



4 Click **OK** to close the **Settings** dialog box.

Adding a blocked site from HostWatch

To add an IP address to the blocked sites list from HostWatch, right-click on the connection and use the pop-up window to select the IP address from the connection to add to the blocked sites list. You must set the time for the IP address to be blocked, and give the configuration passphrase.

Pausing the HostWatch display

You can use the **Pause** and **Continue** icons on the toolbar to temporarily stop and then restart the display. Or, use **File > Pause** and **File > Continue**.

CHAPTER 3

Setting Up Your Firebox

To operate correctly, your Firebox® must have the necessary information to apply your security policy to the traffic that goes through your network. Policy Manager gives you one user interface to configure your security policy. This chapter shows you how to:

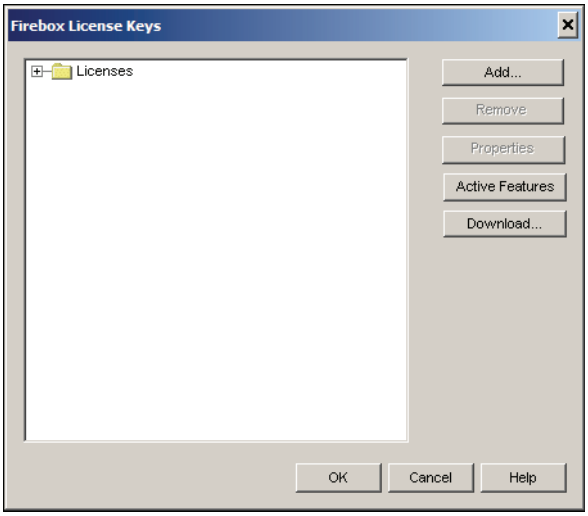
- Add, delete and view licenses
- Use aliases
- Set up a log host
- Configure logging
- Configure Firebox global settings
- Set up the Firebox to use an NTP server
- Configure the Firebox for SNMP

Working with Licenses

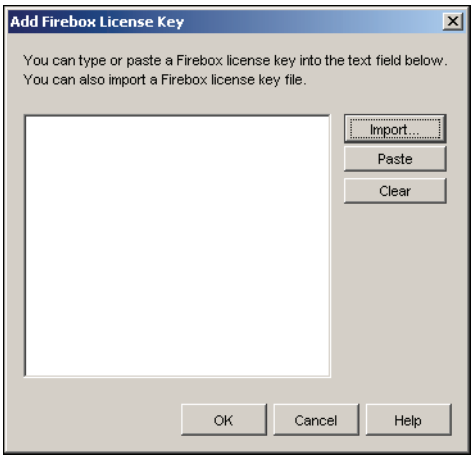
You increase the functionality of your Firebox® when you purchase an option and add the license key to the configuration file. When you get a new key, make sure that you follow the instructions that come with the key. These instructions send you to a Web page where you are prompted to enter the key and the serial number from your Firebox. The Web site creates the license key that you paste into Policy Manager as described in this section.

Adding licenses

1 From Policy Manager, select **Setup > Licensed Features**.
The Firebox License Keys dialog box appears. This dialog box shows the licenses that are available.



2 Click **Add**.
The Add Firebox License Key dialog box appears.



3 Click **Import** and find the license file.
You can also paste the contents of the license file into the dialog box.

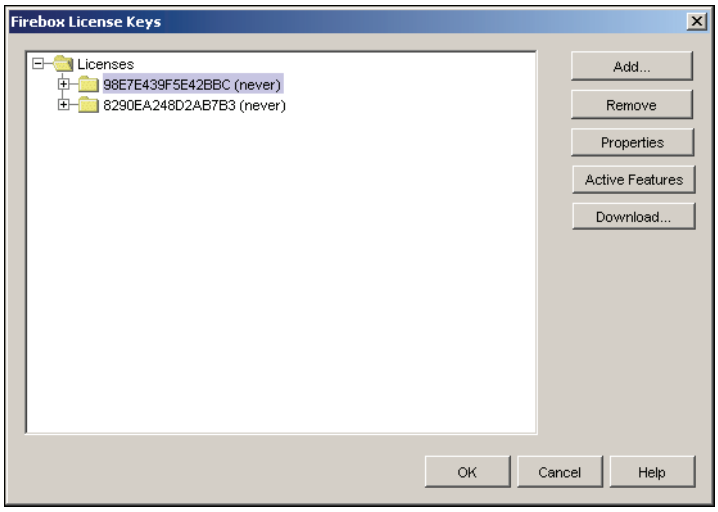
4 Click **OK** two times.
At this time, the features are available on the management station. In many conditions, new dialog boxes and menu commands to configure the feature appear in Policy Manager.

5 Save the configuration to the Firebox.
The feature does not operate on the Firebox until you save the configuration file to the Firebox.

Deleting a license

1 From Policy Manager, select **Setup > Licensed Features**.
The Firebox License Keys dialog box appears.

2 Expand **Licenses**, select the license ID you want to remove, and click **Remove**.

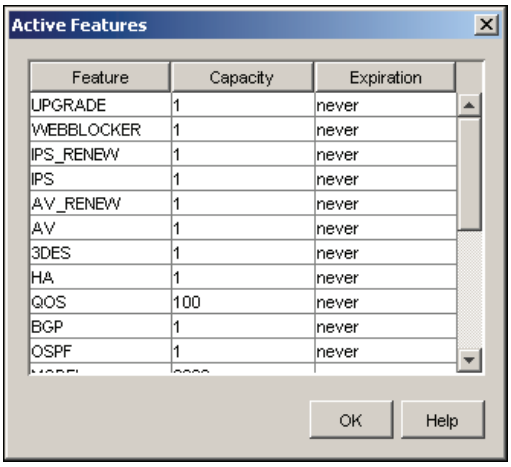


3 Click **OK**.

4 Save the configuration to the Firebox.

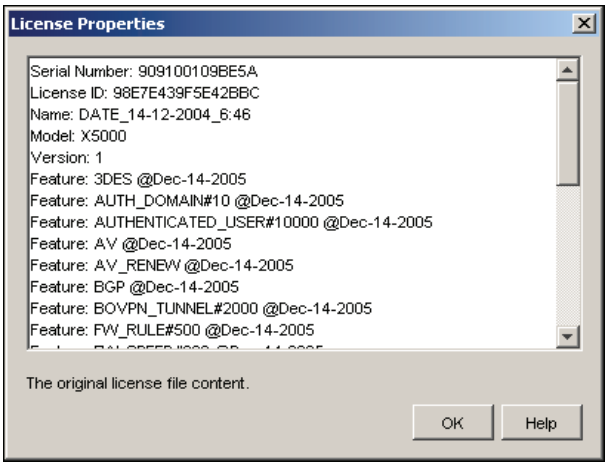
Seeing the active features

To see a list of all features with licenses, select the license key and click **Active Features**. The **Active Features** dialog box shows each feature along with its capacity and expiration.



Seeing the properties of a license

To see the properties of a license, select the license key and click **Properties**. The **License Properties** dialog box shows the serial number of the Firebox to which this license applies, along with its ID and name, the Firebox model and version number, and the available Firebox features.



Downloading a license key

If your license file is not current, you can download a copy of any license file from the Firebox to your management station. To download license keys from a Firebox, select the license key and click **Download**. A dialog box appears for you to type the status passphrase of the Firebox.

Working with Aliases

An alias is a shortcut that identifies a group of hosts, networks, or interfaces. When you use an alias, it is easy to create a security policy because the Firebox® allows you to use aliases when you create policies.

These are some default aliases included in Policy Manager that you can use:

Any-Trusted
: This is an alias for all Firebox interfaces of type "trusted" (as defined in **Policy Manager > Network > Configuration**), and any network you can access through these interfaces.

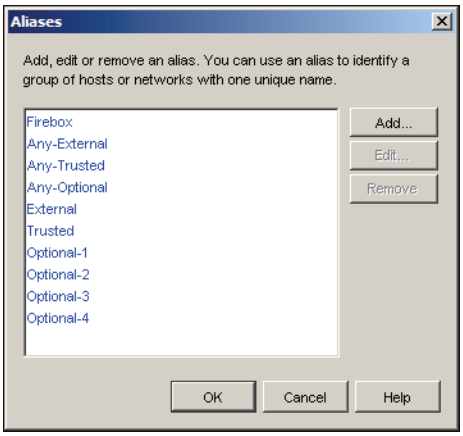
Any-External
: This is an alias for all Firebox interfaces of type "external" (as defined in **Policy Manager > Network > Configuration**), and any network you can access through these interfaces.

Any-Optional
: These are aliases for all Firebox interfaces of type "optional" (as defined in **Policy Manager > Network > Configuration**), and any network you can access through these interfaces.

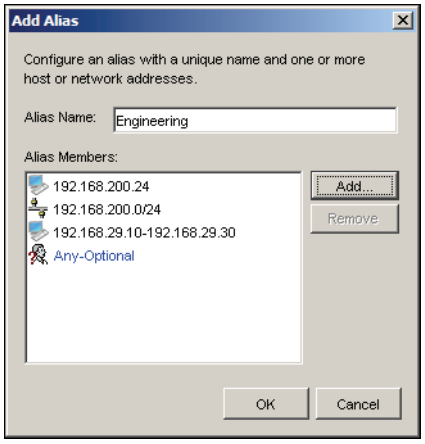
Using an alias is different from using user authentication. With user authentication, you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet tools, for example HTTP or FTP. For more information about user authentication, see "How User Authentication Works" on page 111.

Creating an alias

1 From Policy Manager, select **Setup > Aliases**.
The Aliases dialog box appears.



2 Click **Add**.
The Add Alias dialog box appears.



3 In the **Alias Name** text box, type a unique name to identify the alias.
This name appears in lists when you configure a security policy.
4 Click **Add** to add an IP address, subnet, interface, or a different alias to the list of alias members.
The member appears in the list of Alias Members.
5 Click **OK** two times.

Using Logging

The WatchGuard® System Manager installation utility can install Policy Manager and the WatchGuard Log Server on the same computer. Or, you can also install the Log Server on one or more other computers. You use Policy Manager and the Log Server to set up and manage log messages.

Use Policy Manager to:

- Add the log hosts.
- Change the configuration of policies and packet handling

- Save the configuration file to the Firebox®

Use WatchGuard Log Server to:

- Select the global logging and the notification configuration for the host
- Set the log encryption key on the local log server.

Categories of log messages

The Firebox sends four types of log messages: Traffic, Alarm, Event, and Diagnostic.

Traffic messages

The Firebox sends traffic messages as it applies packet filter and proxy rules to traffic that goes through the Firebox.

Alarm messages

Alarm messages are sent when an event occurs that causes the Firebox to complete an action in response to an event. When the alarm condition occurs, the Firebox sends an alarm message to the Traffic Monitor and the log server, and causes the specified action to occur.

Some alarms are set in your Firebox configuration. For example, you can use Policy Manager to configure an alarm when a specified threshold occurs. Other alarms are set in a default configuration. The Firebox sends an alarm message when a network connection on one of the Firebox interfaces goes down. You cannot change this in your configuration.

There are eight categories of alarm logs: System, IPS, AV, Policy, Proxy, Counter, Denial of service, and Traffic.

Event messages

Event messages are created because of Firebox user actions. Events that cause event messages include:

- Firebox start up/shut down
- Firebox and VPN authentication
- Process start up/shut down
- Problems with the Firebox hardware components
- Any task done by the Firebox administrator

Diagnostic messages

Diagnostic (debug) messages include more information than other messages that the Firebox sends. You can use these messages to help troubleshoot problems. There are 27 different product components that can send diagnostic messages.

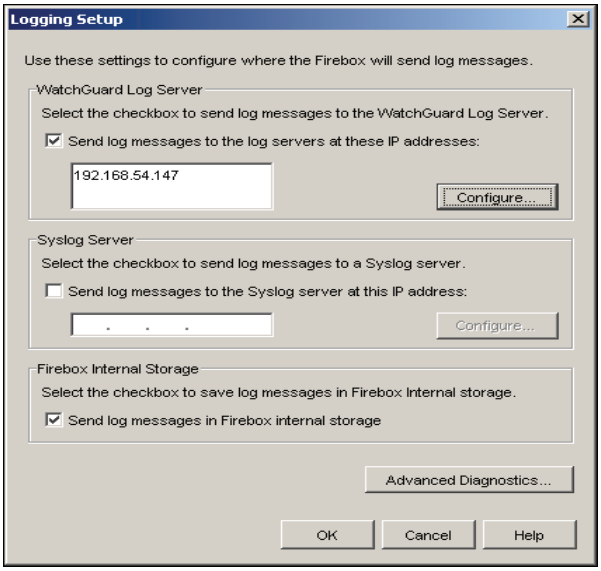
Designating log servers for a Firebox

It is recommended that you have a minimum of one log server to use WatchGuard System Manager. You can select a different primary log server and more than one backup log server.

To set a log server:

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Select the log server or servers you want to use. Click the **Send log messages to the log servers at these IP addresses** check box.


Logging Setup
Use these settings to configure where the Firebox will send log messages.
WatchGuard Log Server
Select the checkbox to send log messages to the WatchGuard Log Server.
Send log messages to the log servers at these IP addresses:
192.168.54.147
Configure...
Syslog Server
Select the checkbox to send log messages to a Syslog server.
Send log messages to the Syslog server at this IP address:
Configure...
Firebox Internal Storage
Select the checkbox to save log messages in Firebox internal storage.
Send log messages in Firebox internal storage
Advanced Diagnostics...
OK
Cancel
Help

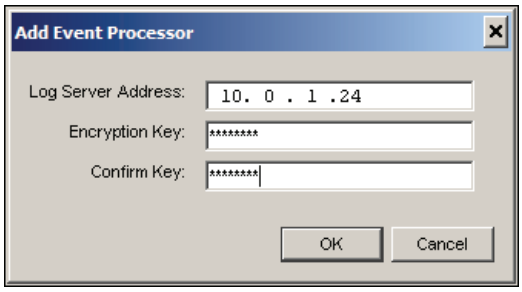
Adding a log server

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Click **Configure**. Click **Add**.
The Add Event Processor dialog box appears.

3 In the **Log Server Address** box, type the IP address of the log server you want to use.

4 In the **Encryption Key** and **Confirm** boxes, type the log server encryption key. The permitted range for the encryption key is 8–32 characters.



5 Click **OK**. Click **OK** to close the **Configure Log Servers** dialog box. Click **OK** to close the **Logging Setup** dialog box.

Setting log server priority

If the Firebox cannot connect to the log server with the highest priority, it connects to the subsequent log server in the priority list. If the Firebox examines each log server in the list and cannot connect, it tries to connect to the first log server in the list again. You can create a priority list for log servers.

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Click **Configure**.
The Configure Log Servers dialog box appears.

3 Select a log server from the list in the **Configure Log Servers** dialog box. Use the **Up** and **Down** buttons to change the order.

Activating Syslog logging

You can configure the Firebox to send log information to a Syslog server. A Firebox can send log messages to a log server and a Syslog server at the same time, or send log messages to one or the other. Syslog log messages are not encrypted. We recommend that you do not select a host on the external interface as the Syslog server because this is not secure.

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Select the **Send Log Messages to the Syslog server at this IP address** check box.

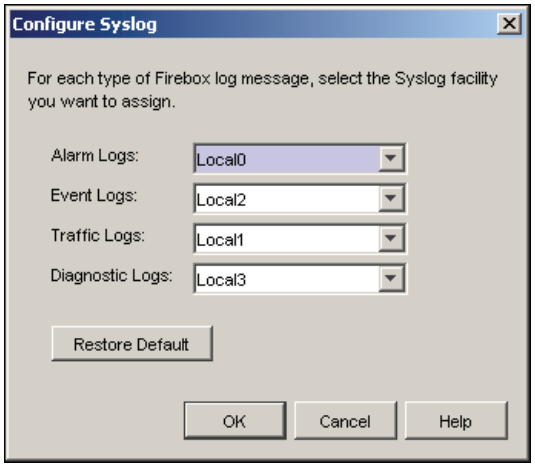
3 In the address box, type the IP address of the Syslog server.

4 Click **Configure**.
The Configure Syslog dialog box appears.

5 For each type of log message, select the Syslog facility to which you want it assigned. For information on types of log messages, see "Categories of log messages" on page 36.
The Syslog facility refers to one of the fields in the Syslog packet and to the file the Syslog is sent to. You can use Local0 for high priority Syslog messages, such as alarms. You can use Local1- Local 7 to assign priorities for other types of log messages (with lower numbers having greater priority).

6 Click **OK**. Click **OK** to close the **Logging Setup** dialog box.

7 Save your changes to the Firebox.

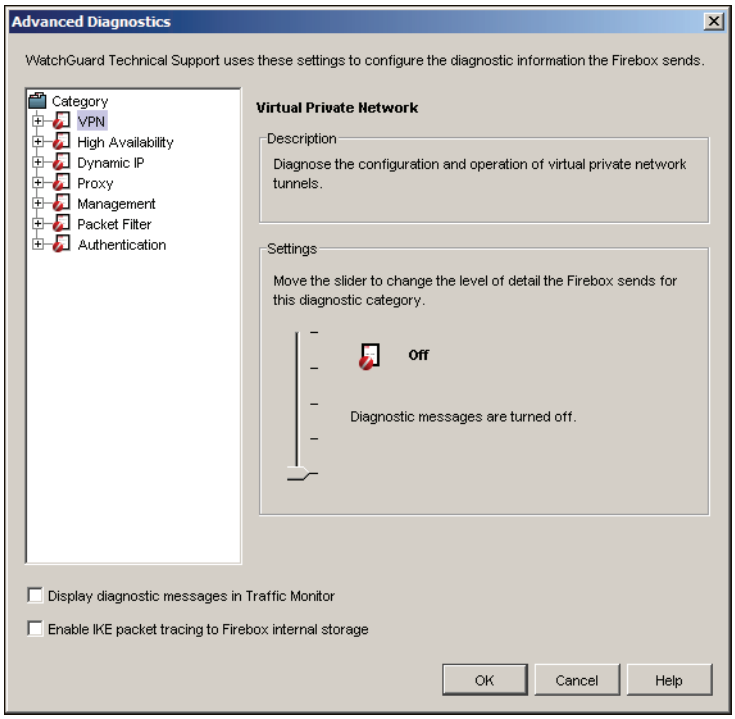


Enabling advanced diagnostics

You can select the level of diagnostic logging to write to your log file or to Traffic Monitor. We do not recommend that you set the logging level to the highest level unless a technical support representative tells you to in order to troubleshoot a problem. It can cause the log file to fill up very quickly.

1 From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.

2 Click **Advanced Diagnostics**.
The Advanced Diagnostics dialog box appears.



3 Select a category from the category list.
A description of the category appears in the Description box.

4 Use the slider below **Settings** to set the level of information that a log of each category includes in its log message. When the lowest level is set, diagnostic messages for that category are turned off.

5 To show diagnostic messages in Traffic Manager, select the **Display diagnostics messages in Traffic Monitor** check box.

6 To have the Firebox collect a packet trace for IKE packets, select the **Enable IKE packet tracing to Firebox internal storage** check box. To see the packet trace information the Firebox collects, start Firebox System Manager, and click the **Status** tab. Click **Support** to have Firebox System Manager get the packet trace information from the Firebox.

Using Global Settings

In Policy Manager you select settings that control the actions of many Firebox® features with the Global Settings tool.

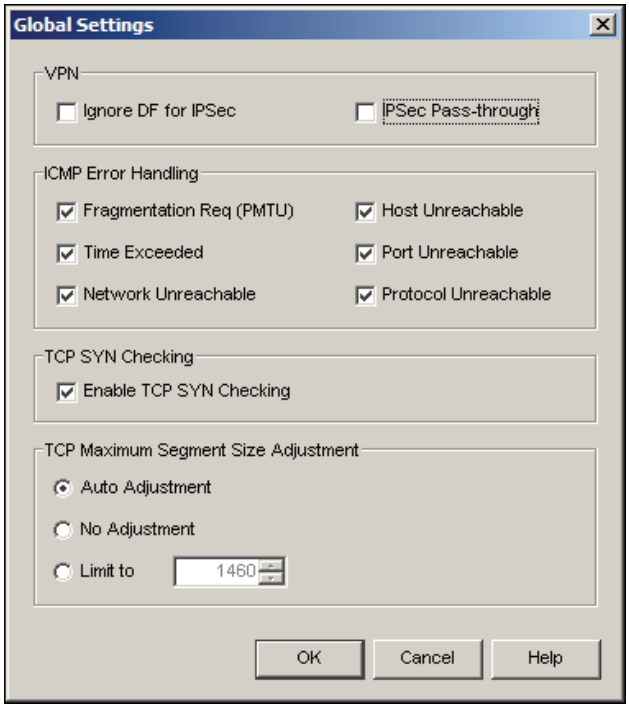
You set basic parameters for:

- VPN

- ICMP error handling
- TCP SYN checking
- TCP maximum size adjustment

1 From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.

2 Configure the different categories of global settings as shown in the sections below.



VPN

The global VPN settings are:

Ignore DF for IPSec

Ignore the setting of the **Don't Fragment** bit in the IP header.

IPSec pass through

If a user must make IPSec connections to a Firebox from behind a different Firebox, you must enable the **IPSec Pass-through** check box. For example, if mobile employees are at a customer location that has a Firebox, they can make IPSec connections to their network using IPSec. For the local Firebox to correctly allow the outgoing IPSec connection, you must add an IPSec policy to Policy Manager.

ICMP error handling

Internet Control Message Protocol (ICMP) controls errors during connections. It is used for two types of operations:

- To tell about error conditions.
- To probe a network to find general characteristics about the network.

The Firebox sends an ICMP error message each time an event occurs that matches one of the parameters you selected. The global ICMP error handling parameters and their descriptions are:

Fragmentation req (PMTU)
The IP datagram must be fragmented, but this is prevented because the Don't Fragment bit in the IP header is set.

Time exceeded
The datagram was dropped because the Time to Live field expired.

Network unreachable
The datagram could not get to the network.

Host unreachable
The datagram could not get to the host.

Port unreachable
The datagram could not get to the port.

Protocol unreachable
The protocol piece of the datagram can not be delivered.

TCP SYN checking

The global TCP SYN checking setting is:

Enable TCP SYN checking
This feature makes sure that the TCP three-way handshake is done before the Firebox allows a data connection.

TCP maximum segment size adjustment

The TCP segment can be set to a specified size for a connection that must have more TCP overhead (like PPPoE, ESP, AH, and so on). If this size is not correctly configured, users cannot get access to some Web sites. The global TCP maximum segment size adjustment settings are:

Auto adjustment
The Firebox examines all maximum segment size (MSS) negotiations and changes the MSS value to the applicable one.

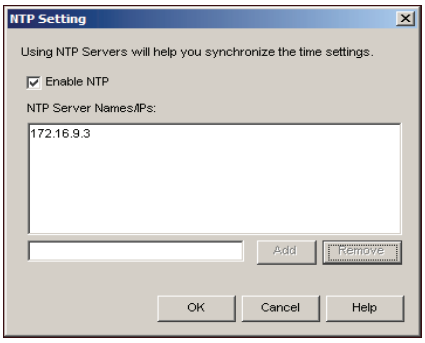
No adjustment
The Firebox does not change the MSS.

Limit to
You set a size adjustment limit.

Setting NTP Servers

Network Time Protocol (NTP) synchronizes computer clock times across a network. NTP operates on TCP and UDP port 123. The Firebox® can synchronize its clock to an internet NTP server to help you keep all devices on your network synchronized to the same time.

1 From Policy Manager, select **Setup > NTP**.



2 Select the **Enable NTP** check box.

3 In the box below the **NTP Server Names/IPs** list, type the IP addresses of the NTP servers you want to use, and then click **Add**.
The Firebox can use up to three NTP servers.

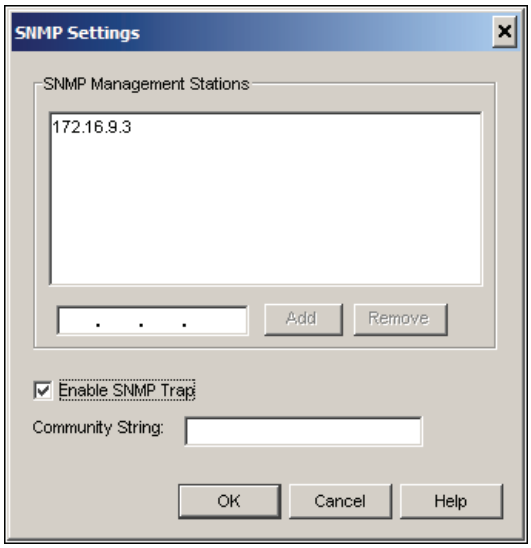
4 Click **OK**.

Working with SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing networks. SNMP uses management information bases (MIBs) that have management information that is available from network devices. With Fireware appliance software, the Firebox supports SNMPv1 and SNMPv2c.

You can configure the Firebox® as an SNMP device. It can then receive SNMP polls from an SNMP server.

1 From Policy Manager, select **Setup > SNMP**.



2 In the box below the **SNMP Management Stations** list, type the IP address of the SNMP server, and then click **Add**.

3 To enable the Firebox to send SNMP traps, select the **Enable SNMP Trap** check box. You must also edit the policy that will trigger a trap. Open a policy configuration for edit and select the **Properties** tab. Click **Logging** and select the **Enable SNMP Trap** check box .
An SNMP trap is an event notification the Firebox sends to the SNMP management system. The trap identifies when a condition occurs, such as a value that is more than its predefined threshold.

4 Type the **Community String** the Firebox must use when connecting to the SNMP server.
The community string is like a user ID or password that allows access to the statistics of a device. This community string must be included with all SNMP requests. If the community string is correct, the device gives the requested information. If the community string is not correct, the device discards the request and does not respond.

5 Click **OK**.

Using MIBs

WatchGuard System Manager with Fireware appliance software supports two types of Management Information Bases (MIBs):

- Public MIBs, including IETF standards and MIB2
- Private MIBs, such as those created by WatchGuard

When you install WatchGuard System Manager, MIBs are placed in My Documents\My WatchGuard\Shared WatchGuard\SNMP.

The Firebox supports these read-only object MIBs:

- RFC1155-SMI
- SNMPv2-SMI
- RFC1213-MIB
- RAPID-MIB
- RAPID-SYSTEM-CONFIG-MIB

CHAPTER 4

Basic Firebox Configuration

After your Firebox® is installed on your network and operates with a basic configuration file, you can start to add custom configuration settings to align with your organization requirements. This chapter shows you how to do some basic configuration and maintenance tasks. Some of these tasks you complete many times as you work with your Firebox. Other tasks you complete only do one time.

These basic configuration tasks include:

- Open a configuration file on a local computer or from the Firebox
- Save a configuration file to a local computer or the Firebox
- Change the Firebox passphrases
- Set the Firebox time zone
- Give the Firebox a name to use (instead of an IP address)
- Set basic schedules to use in your policies later

Opening a Configuration File

Policy Manager for Fireware is a software tool that lets you make, change, and save configuration files. A configuration file, with the extension `.xml`, includes all configuration data, options, addresses, and other information that makes up your Firebox® security policy. When you use Policy Manager, you see a version of your configuration file that is easy to examine and change.

When you work with a configuration file, you can:

- Open the current configuration file on your Firebox
- Open a configuration file saved on your local hard drive
- Make a new configuration file

Opening a working configuration file

A common task for a network administrator is to make a change to your current security policy. For example, your business purchases a new software application, and you must open a port and protocols to a server at a vendor location. For this task, you must change your configuration file with Policy Manager.

Using WatchGuard System Manager

1 From the Windows desktop, click **Start > All Programs > WatchGuard System Manager 8.2 > WatchGuard System Manager**.
WatchGuard System Manager 8.2 is the default name of the folder for the Start menu icons. You can change this folder name during installation.

2 From WatchGuard System Manager, select **File > Connect To Device**.

Or,
click the Connect to Device icon on the WatchGuard System Manager toolbar. The Connect to Firebox dialog box appears.

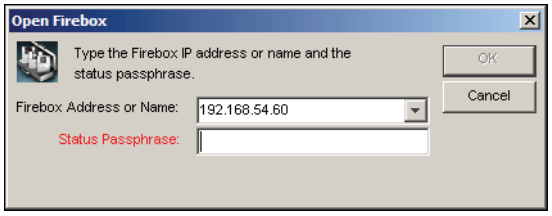
3 Use the drop-down list to select your Firebox, or type its trusted IP address. Type the status passphrase. Click **OK**.
The device appears in the WatchGuard System Manager Device Status tab.

4 Select the Firebox on the **Device Status** tab. Then, select **Tools > Policy Manager**.

Or,
click the Policy Manager icon on the WatchGuard System Manager toolbar. Policy Manager opens, and it puts the configuration file in use on the selected Firebox.

Using Policy Manager

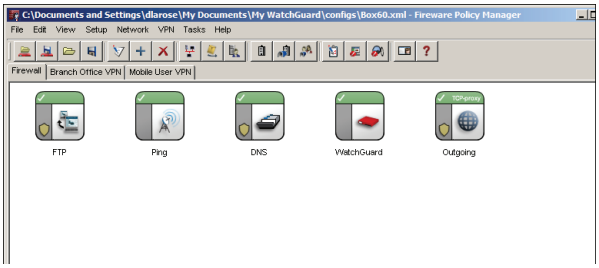
1 From Policy Manager, click **File > Open > Firebox**.
The Open Firebox dialog box appears.
If you get an error message that tells you that you cannot connect, try again.



2 From the **Firebox Address or Name** drop-down list, select a Firebox.
You can also type the IP address or host name.

3 In the **Passphrase** text box, type the Firebox status (read-only) passphrase.
Use the status passphrase here. You must use the configuration passphrase to save a new configuration to the Firebox.

4 Click **OK**.
Policy Manager opens the configuration file and shows the settings.



If you cannot open Policy Manager, try these steps:

- If the **Connect to Firebox** dialog box immediately comes back after you enter the passphrase, make sure that Caps Lock is off and that you type the passphrase correctly. Remember that the passphrase is case-sensitive.
- If the **Connect to Firebox** dialog box times out, make sure that you have a link on the trusted interface and on your computer. Make sure that you typed the correct IP address for the trusted interface of the Firebox. Also make sure that your computer IP address is in the same network as the trusted interface of the Firebox.

Opening a local configuration file

Some network administrators find it helps to save more than one version of a Firebox configuration file. For example, if you have a new security policy to use, we recommend that you save the old configuration file to a local hard drive first. Then if you do not want the new configuration, you can restore the old version. You can open configuration files that are on any network drive to which your management station can connect.

1 From WatchGuard System Manager, select **Tools > Policy Manager** (or click the Policy Manager icon).

2 Select **File > Open > Configuration File**.

Or,
click the Open File icon on the Policy Manager toolbar. A standard Windows open file dialog box appears.

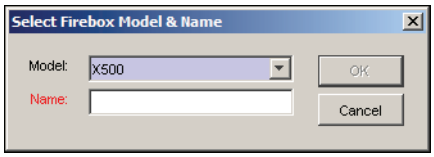
3 Use the **Open** dialog box to find and to select the configuration file. Click **Open**.
Policy Manager opens the configuration file and displays the settings.

Making a new configuration file

The Quick Setup Wizard makes a basic configuration file for your Firebox. We recommend that you use this as the base for each of your configuration files. You can also use Policy Manager to make a new configuration file with only the default configuration properties.

1 From WatchGuard System Manager, select **Tools > Policy Manager** (or click the Policy Manager icon).

2 From Policy Manager, select **File > New**.
The Select Firebox Model and Name dialog box appears.



3 Use the **Model** drop-down list to select your Firebox model. Because there are features that match each model, it is important that you select the same model as your hardware device.

4 Type a name for the Firebox.

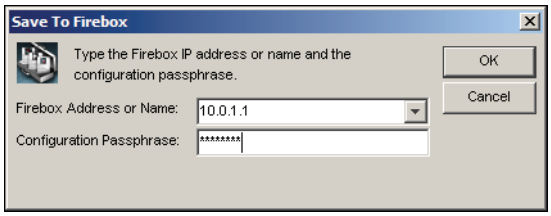
5 Click **OK**.
Policy Manager makes a new configuration with the file name <name>.xml, where <name> is the name you gave the Firebox.

Saving a Configuration File

After you make a new configuration file or change the current configuration file, you can save it directly to the Firebox®. You can also save it to a local hard disk.

Saving a configuration to the Firebox

1 From Policy Manager, click **File > Save > To Firebox.**
The Save to Firebox dialog box appears.



2 From the **Firebox Address or Name** drop-down list, select a Firebox.
When you type an IP address, type all the numbers and the periods. Do not use the TAB key or arrow key.

3 Type the Firebox configuration passphrase. You must use the configuration passphrase to save a file to the Firebox.

4 Click **OK.**

Saving a configuration to a local hard drive

1 From Policy Manager, click **File > Save > As File**.
You can also use CTRL-S. A standard Windows save file dialog box appears.

2 Type the name of the file.
The default procedure is to save the file to the WatchGuard® directory. You can also browse to any folder to which you can connect from the management station. For better security, we recommend that you save the files in a safe folder with no access to other users.

3 Click **Save**.
The configuration file saves to the local hard drive.

About Firebox Backup Images

A Firebox backup image is an encrypted and saved copy of the operating image from the Firebox flash disk. It includes the Firebox appliance software and configuration file. You can save a backup image to your management station or to a directory on your network. We recommend that you regularly make back ups of the Firebox image. We also recommend that you to create a backup image of the Firebox before you make significant changes to your Firebox configuration or upgrade your Firebox or its appliance software.

Creating a Firebox backup image

1 From Policy Manager, select **File > Backup**.

2 Type the configuration passphrase for your Firebox.

3 Type and confirm an encryption key.
This key is used to encrypt the backup file. If you lose or forget this encryption key, you will not be able to restore the backup file.

4 Select the directory in which to save the backup file.
The default location for a backup file with a ".fxi" extension is C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address> - <date>.fxi.

Restoring a Firebox backup image

1 From Policy Manager, select **File > Restore**.
2 Type the configuration passphrase for your Firebox.
3 Type the encryption key you used when you created the backup image.
The Firebox restores the backup image and restarts. It uses the backup image on restart.

Changing the Firebox passphrases

A Firebox® uses two passphrases:

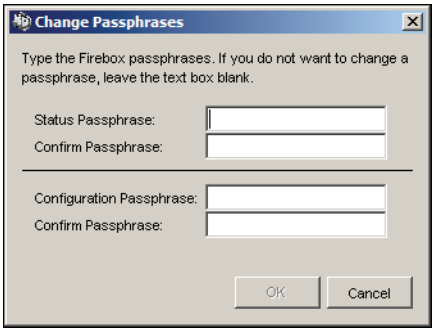
- Status passphrase
  The read-only password that allows access to the Firebox
- Configuration passphrase
  The read-write password that allows an administrator full access to the Firebox

To create a secure passphrase, we recommend that you:

- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language. Make a new acronym that only you know.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.
- Use a selection of uppercase and lowercase characters, numbers, and special characters (for example, Im4e@tiN9).

An additional security measure is to change the Firebox passphrases at regular intervals. To do this, you must have the configuration passphrase.

1 From Policy Manager, open the configuration file on the Firebox.
2 Click **File > Change Passphrases**.
An Open Firebox dialog box appears.
3 From the **Firebox** drop-down list, select a Firebox or type the IP address or name of the Firebox. Type the Firebox configuration (read/write) passphrase. Click **OK**.
The Change Passphrases dialog box appears.



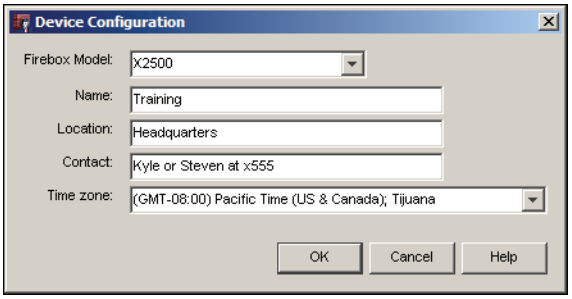
4 Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase.
5 Click **OK**.
The new flash image and the new passphrases save to the Firebox. The Firebox automatically starts again.

Setting the Time Zone

The Firebox® time zone controls the date and time that appear in the log file and on tools that include LogViewer, Historical Reports, and WebBlocker. Set the Firebox time zone to the time zone for the physical location of the Firebox. This time zone setting allows for the time to appear correctly in the log messages. The Firebox system time is set to Greenwich Mean Time (GMT) by default.

1 From Policy Manager, click **Setup > System**.
The Device Configuration dialog box appears.

2 From the **Time zone** drop-down list, select the time zone you want. Click **OK**.

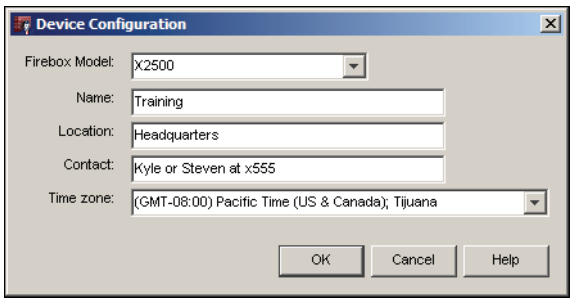


Setting a Firebox Friendly Name

You can give the Firebox® a special name to use in your log files and reports. If you do not do this procedure, the log files and reports use the IP address of the Firebox external interface. Many customers use a Fully Qualified Domain Name if they register such a name with the DNS system. You must give the Firebox a special name if you use the Management Server to configure VPN tunnels and certificates with the Firebox.

1 From Policy Manager, click **Setup > System**.
The Device Configuration dialog box appears.

2 In the **Name** text box, type the special name you want for the Firebox. Click **OK**.
You can use all characters but spaces and slashes (/ or \).

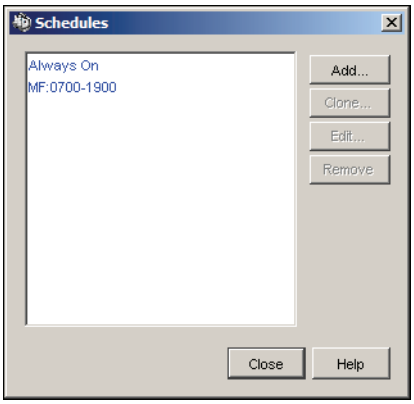


Creating Schedules

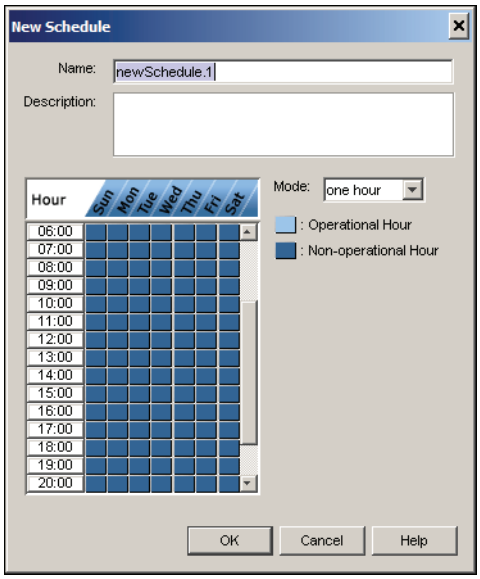
You can use schedules to automate some Firebox® actions such as WebBlocker tasks. You can create a schedule for each day of the week, or create a different schedule for each day of the week. You can then

use these schedules in policies that you create. For information on how to use schedules in policies, see the "Configuring Policies" chapter.

1 From Policy Manager, select **Setup > Actions > Schedules**.
The Schedules dialog box appears.



2 Click **Add**.
The New Schedule dialog box appears.



3 Type a schedule name and description. The schedule name appears in the **Schedule** dialog box. Make sure that the name is easy to remember.

4 From the **Mode** drop-down list, select the time increment for the schedule: one hour, 30 minutes, or 15 minutes.
The chart on the left of the New Schedule dialog box reflects your entry in the drop-down list.

5 The chart in the dialog box shows days of the week along the x-axis (horizontal) and increments of the day on the y-axis (vertical). Click boxes in the chart to change them between operational hours (when the policy is active) and non-operational hours (when the policy is not in effect).

6 Click **OK** to close the **New Schedule** dialog box. Click **Close** to close the **Schedules** dialog box.

To edit an existing schedule, select the schedule name in the **Schedule** dialog box and click **Edit**.
To create a new schedule from an existing one, select the schedule name and click **Clone**.

CHAPTER 5

Network Setup and Configuration

When you install the Firebox® in your network and complete the Quick Setup Wizard, you have a basic configuration file. You then use Policy Manager to make a new configuration file or to change the one you made with the Quick Setup Wizard.

If you are new to network security, we recommend that you do all the procedures in this chapter to make sure you configure all the components of your network. In this chapter, you learn how to use Policy Manager to:

- Make a new configuration file
- Configure the Firebox interfaces
- Add a secondary network
- Add DNS and WINS server information
- Configure network and host routes

Making a New Configuration File

The first step to start a new configuration file is to connect to a Firebox® and open Policy Manager. There are two methods to do this.

Note

We recommend that you create a new configuration file only after a fresh install or a safe mode restart.

Connecting to the Firebox from WSM

1 From WatchGuard® System Manager, select **File > Connect To > Device**.

Or,
click the Connect to Device icon on the WatchGuard System Manager toolbar. The Connect to Firebox dialog box appears.

2 Use the drop-down list to select your Firebox, or type its trusted IP address. Type the status passphrase. Click **OK**.
The device appears in the WatchGuard System Manager Device tab.

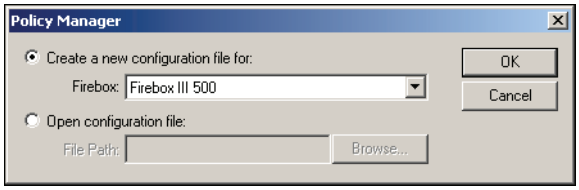
3 Select the Firebox on the **Device** tab. Then, select **Tools > Policy Manager**.

Or,
Click the Policy Manager icon on the WatchGuard System Manager toolbar. Policy Manager opens, and it opens the configuration file in use on the selected Firebox.

Connecting to the Firebox from Policy Manager

1 From WatchGuard System Manager, select **Tools > Policy Manager**.

Or,
click the Policy Manager icon on the WatchGuard System Manager toolbar. The Policy Manager dialog box appears.



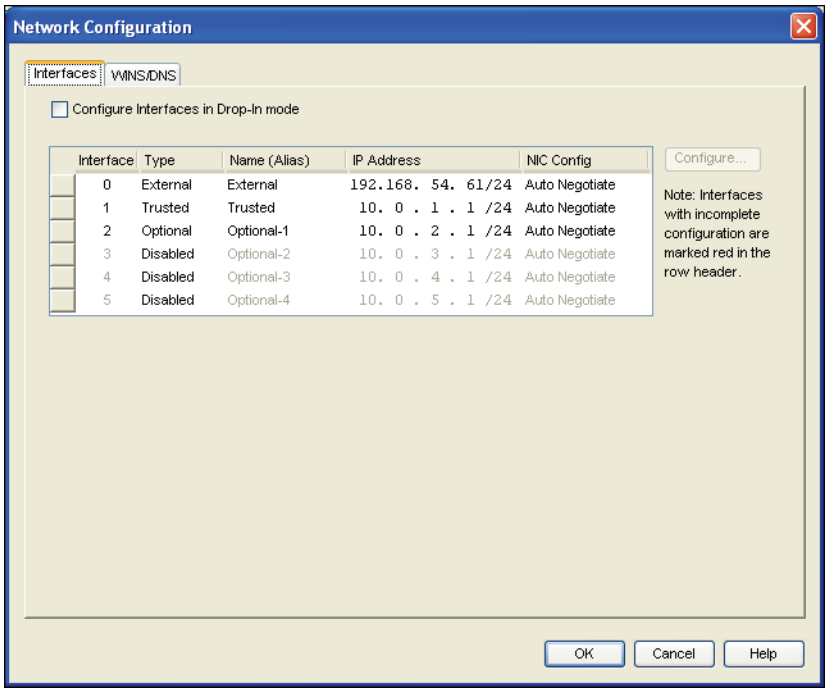
2 Use the Firebox drop-down list to select the model of Firebox to which you are connected. Click **OK**. The new configuration file contains the default parameters for the specified Firebox model.

Note

We recommend that you save the configuration file frequently. Select **File > Save > As File**..

Changing Firebox Interface IP Addresses

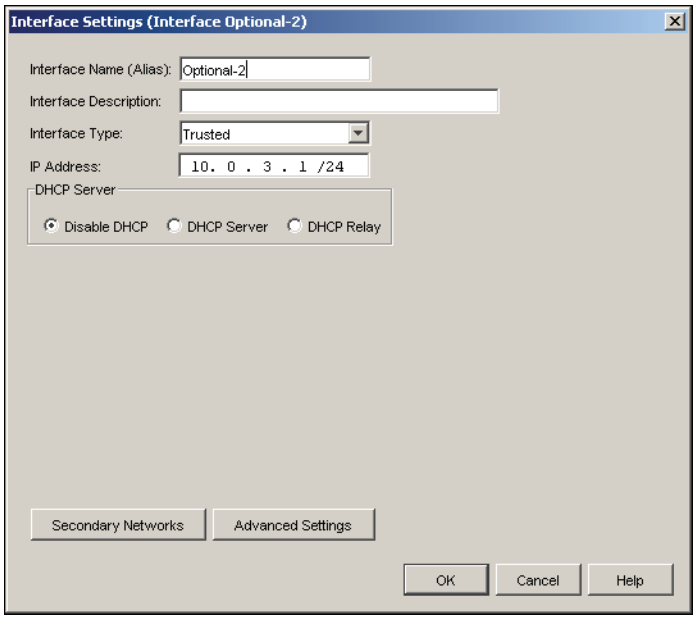
1 From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.


Network Configuration
Interfaces
VWINS/DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
0 External External 192.168. 54. 61/24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 Disabled Optional-2 10. 0 . 3 . 1 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
Configure...
Note: Interfaces with incomplete configuration are marked red in the row header.
OK
Cancel
Help

2 Select the interface you want to configure. Click **Configure**.
The Interface Settings dialog box appears.

3 (Optional) Type a description of the interface in the **Interface Description** field.

4 You can change the interface type from the **Interface Type** drop-down list.



5 You can change the interface IP address. Type the IP address in slash notation.
When you type an IP addresses, type all the numbers and the periods. Do not use the TAB or arrow key.

6 If you are configuring a trusted or optional interface, select **Disable DHCP**, **DHCP Server**, or **DHCP Relay**.
See "Configuring the Firebox as a DHCP server" for the DHCP server option, and see "Configuring a DHCP relay" on page 56 for the DHCP relay option. If you are configuring the external interface, see "Configuring the external interface" on page 56.

7 Click **OK**.

Configuring the Firebox as a DHCP server

Dynamic Host Configuration Protocol (DHCP) is an Internet Protocol that makes it easier to control a large network. A computer you configure as the DHCP server automatically gives IP addresses to the computers on your network. You set the range of addresses. You can configure the Firebox® as a DHCP server for networks behind the firewall.

If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.

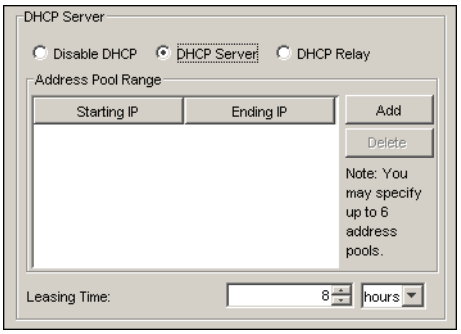
1 Select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Select the trusted or an optional interface.

3 Click **Configure** and select **DHCP Server**.

4 To add an IP address range, click **Add** and type the first and last IP addresses.
You can configure a maximum of six address ranges.

5 Use the arrow buttons to change the **Default Lease Time**.
This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client sends data to the DHCP server to get a new lease.



Configuring a DHCP relay

One method to get IP addresses for the computers on the Firebox trusted or on an optional network (or through a VPN tunnel) is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different location than the DHCP client. When the Firebox gets the reply, it sends it to the computers on the Firebox trusted or optional network. This option lets computers in more than one office use the same network address range.

1 Select **Network > Configuration**.
The Network Configuration dialog box appears.
2 Select the trusted or an optional interface.
3 Click **Configure** and click **DHCP Relay**.
4 Type the IP address of the DHCP server in the related field. Make sure to add a route to the DHCP server, if necessary.
5 Click **OK.** You must restart the Firebox to complete the change.

Configuring the external interface

The Firebox can get a dynamic IP address for the external interface with Dynamic Host Configuration Protocol (DHCP) or PPPoE (Point-to-Point Protocol over Ethernet). With DHCP, the Firebox uses a DHCP server that is controlled by your Internet Service Provider (ISP) to get an IP address, gateway, and netmask. With PPPoE, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. Fireware™ supports unnumbered and static PPPoE. This connection automatically configures your IP address, gateway, and netmask. If you configure your external interface using DHCP or PPPoE, you cannot add external secondary networks or use external aliases in Policy Manager.

Note

If you configure more than one interface as an external interface, only the lowest-order external interface can serve as an IKE gateway or an IPSec tunnel endpoint. If this interface is down, all IPSec tunnels to and from the Firebox will not operate.

Using a static IP address

1 From the **Interface Settings** dialog box, select **Static**.

2 Type the IP address of the default gateway.

3 (Optional) Configure aliases. For more information, see “Working with Aliases” on page 34.

4 Click **OK**.

Using PPPoE

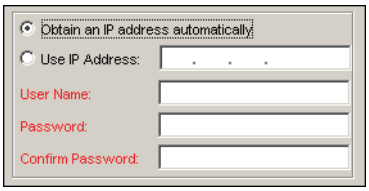
1 From the **Interface Settings** dialog box, select **PPPoE**.

2 Select one of the two options:

- Get an IP address automatically
- Use IP address (supplied by your network administrator).

3 If you selected **Use IP Address**, enter the IP address in the text box to the right.

4 Type the **User Name** and **Password**. You must type the password two times.

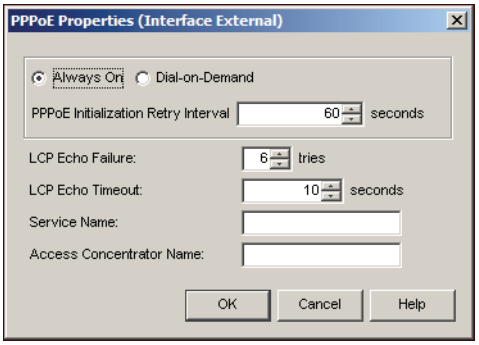


5 Click **Property** to configure PPPoE parameters.

The PPPoE parameters dialog box appears. Your ISP can tell you if it is necessary to change the time-out or LCP values.

6 Use the radio buttons to select when the Firebox connects with the PPPoE server.

- **Always On** — The Firebox keeps a constant PPPoE connection. It is not necessary that network traffic go through the external interface.
- **Dial-on-Demand** — The Firebox connects to the PPPoE server only when it gets a request to send traffic to an IP address on the external interface. If your ISP regularly resets the connection, select Dial-on-Demand. If you do not select Dial-on-Demand, you must manually restart the Firebox each time the connection resets.



7 In the **PPPoE initialization time** field, use the arrows to set the time allowed to start a PPPoE connection.

8 In the **LCP echo failure** field, use the arrows to set the number of failed LCP echo requests allowed before the PPPoE connection is closed.

9 In the **LCP echo timeout** field, use the arrows to set the length of time, in seconds, that the response to each echo time-out must be received.

Using DHCP

1 From the **Interface Settings** dialog box, select **DHCP**.

2 In the **Host Name** text box, type the name of the DHCP server.

Note

If you configure more than one external interface on a Firebox, map the Fully Qualified Domain Name to the external interface IP address of the lowest order.

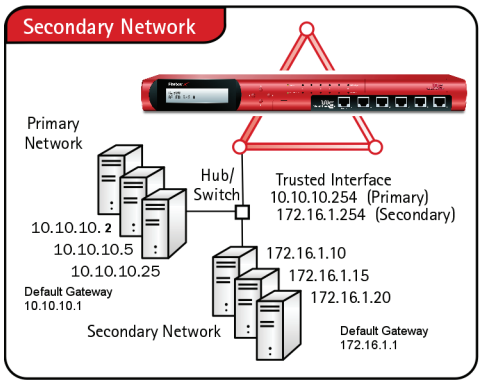
Using more than one external interface

You can configure a Firebox with a maximum of four external interfaces, but VPN tunnels only go through the lowest-order external interface. When you add the Firebox to the Management Server, all of the IP address properties must match the properties of the lowest-order interface. For example, if the interface uses a static IP address, you must configure the Management Server with the same IP address as the lowest-order external interface.

The default configuration sets eth0 as the lowest-order external interface. If you change the interface type, a different interface can be the lowest-order external interface. For example, if you change eth0 from an external interface to a trusted or optional interface. The interface you set as external becomes the lowest-order interface.

Adding Secondary Networks

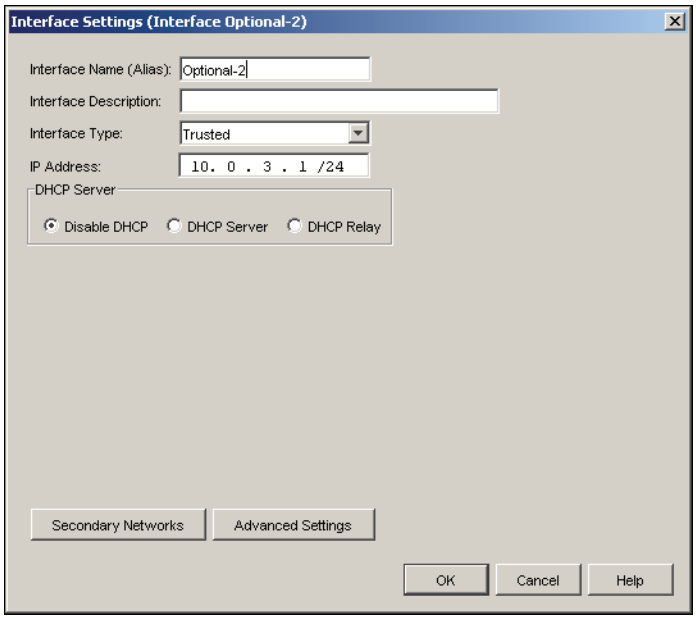
When you add a secondary network, you make a route from an IP address from the secondary network to the IP address of the Firebox® interface. Thus, you make (or add) an IP alias to the interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network also tells the Firebox that there is one more network on the Firebox interface.



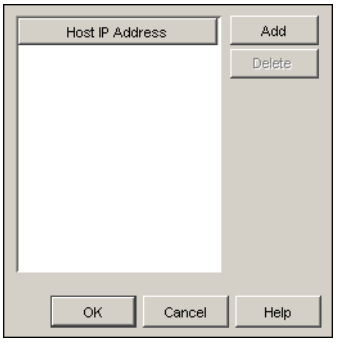
To use Policy Manager to configure a secondary network:

1 Select **Network > Configuration**.
The Network Configuration dialog box appears.

2 Select the interface for the secondary network and click **Configure**.
The Interface Settings dialog box appears.



3 Click **Secondary Networks**.
The Secondary Networks dialog box appears.



4 Click **Add**. Type an unassigned IP address from the secondary network.
When you type IP addresses, type all the numbers and the stops. Do not use the TAB or arrow key.

5 Click **OK**. Click **OK** again.

Note

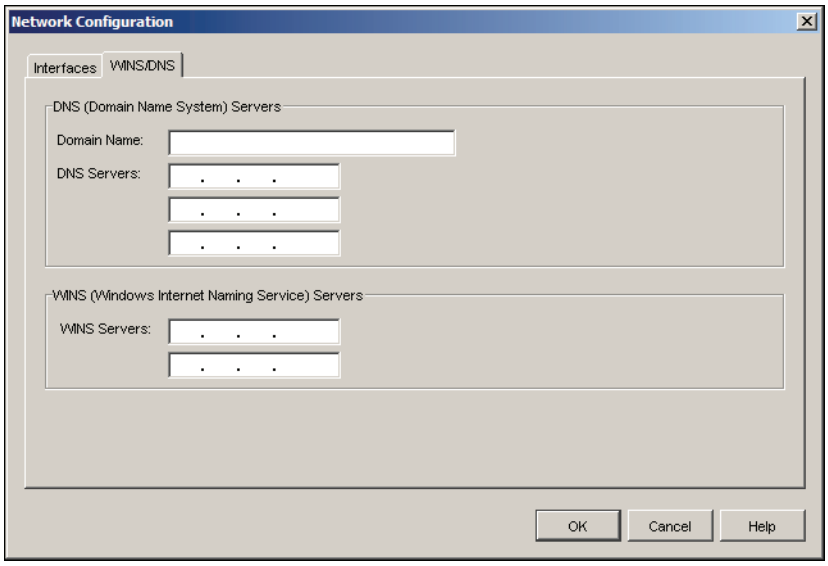
Be careful to add secondary network addresses correctly. Policy Manager does not tell you if the address is correct. We recommend that you do not create a subnet as a secondary network on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network cannot operate correctly.

Adding WINS and DNS Server Addresses

A number of the features of the Firebox® must have shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses. These features include DHCP and Remote User VPN. Access to these servers must be available from the trusted interface of the Firebox.

Make sure that you use only an internal WINS and DNS server for DHCP and Remote User VPN. This helps to make sure that you do not make policies that have configuration properties that prevent users from connecting to the DNS server.

1 From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab.
The WINS/DNS tab appears.



2 Type the primary and secondary addresses for the WINS and DNS servers. If necessary, type a domain name for the DNS server.

Configuring Routes

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

The Firebox® lets you create static routes to send traffic from its interfaces to a router. The router can then send the traffic to the correct destination from the specified route.

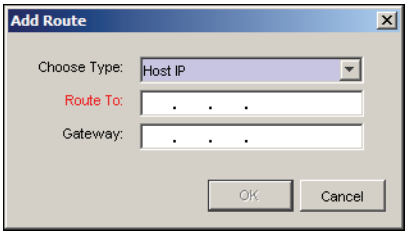
The WatchGuard® Users Forum is also a good source of data about network routes and routers. Use your LiveSecurity service to find more information.

Adding a network route

Add a network route if you have a full network behind a router on your local network. Type the network IP address, with slash notation.

1 From Policy Manager, select **Network > Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.



3 Select **Network IP** from the drop-down list.

4 In the **Route To** text box, type the network address. Use slash notation.
For example, type 10.10.1.0/24.

5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is on one of the same networks as the Firebox.

6 Click **OK** to close the **Add Route** dialog box.
The Setup Routes dialog box shows the configured network route.

7 Click **OK** again to close the **Setup Routes** dialog box.

Adding a host route

Add a host route if there is only one host behind the router or you want traffic to go to only one host. Type the IP address of that specified host, with no slash notation.

1 From Policy Manager, select **Network > Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.

3 Select **Host IP** from the drop-down list.

4 In the **Route To** text box, type the host IP address.

5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is on one of the same networks as the Firebox.

6 Click **OK** to close the **Add Route** dialog box.
The Setup Routes dialog box shows the configured host route.

7 Click **OK** again to close the **Setup Routes** dialog box.

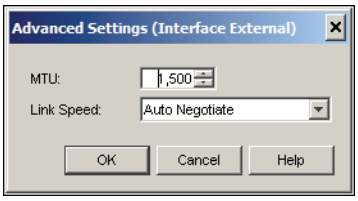
Setting Firebox Interface Speed and Duplex

You can configure the speed and duplex parameters for Firebox® interfaces to automatic or manual configuration. We recommend you set the speed and duplex parameters to match the device the Firebox

connects to. Use the manual configuration option when you must override the automatic Firebox interface parameters to operate with other devices on your network.

1 Select **Network > Configuration**. Click the interface you want to configure, then click **Configure**.

2 Click **Advanced Settings**.
The Advanced Settings dialog box appears.



3 From the **MTU** value control, select the maximum packet size, in bytes, that can be sent through the interface.
A typical value is 1,500 bytes.

4 From the **Link Speed** drop-down list, select **Auto Negotiate** or one of the half-duplex or full-duplex speeds.

5 Click **OK** to close the **Advanced Settings** dialog box. Click **OK** again to close the **Network Configuration** dialog box.

CHAPTER 6

Configuring Policies

In Policy Manager, there are two categories of policies: packet filters and proxies.

A *packet filter* examines each packet's IP header and is the most basic feature of a firewall. It controls the network traffic in to and out of your Firebox®. If the packet header information is legitimate, then the firewall allows the packet. If the packet header information is not legitimate, the Firebox drops the packet. It can also record a log message or send an error message to the source.

A *proxy* uses the same procedure to examine the header information as a packet filter, but it also examines the content. If the content does not match the criteria you set, it denies the packet. A proxy operates at the application layer, while a packet filter operates at the network and transport protocol layers. When you activate a proxy, the Firebox:

- Removes all the network data
- Examines the contents for RFC compliance and content type
- Adds the network data again
- Sends the packet to its destination

A proxy uses more resources and bandwidth than a packet filter. But, a proxy looks for dangerous content that a packet filter cannot find.

In this guide, we refer to packet filters and proxies together as policies. Unless we tell you differently, the procedures refer to both proxies and packet filters.

Policy Manager shows each packet filter and proxy as an icon. The traffic is allowed or denied, and you can configure the source and destination. You also set rules for logging and notification and configure the ports, protocols, and other parameters of the packet filter or proxy.

WatchGuard® Fireware™ includes many pre-configured packet filters and proxies. For example, if you want a packet filter for all Telnet traffic, you add a Telnet packet filter. You can also make a custom packet filter for which you set the ports, protocols, and other parameters.

Creating Policies for your Network

The security policy of your organization is a set of rules that define how you protect your computer network and the information that goes through it. The Firebox® denies all packets that are not specially approved. This security policy helps to protect your network from:

- Attacks that use new or different IP protocols
- Unknown applications

When you configure the Firebox with the Quick Setup Wizard, you set only the basic policies (DNS client, FTP, and TCP outgoing proxy) and interface IP addresses. If you have more software applications and network traffic for the Firebox to examine, you must:

- Configure the policies on the Firebox to let necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

We recommend that you set limits on outgoing access when you configure your Firebox.

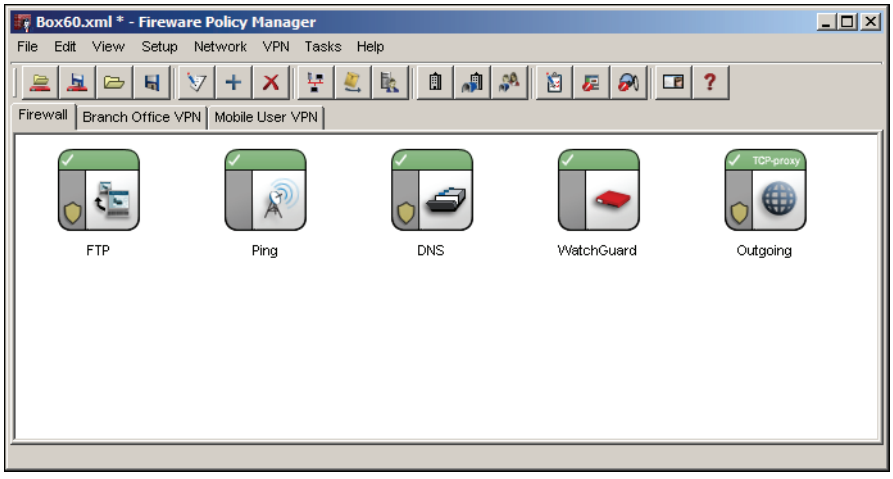
Adding Policies

You add policies with Policy Manager. Policy Manager shows icons or a list to identify the policies that you configure on the Firebox®. For each policy you can:

- Set allowed traffic sources and destinations
- Make filter rules and policies
- Enable or disable the policy
- Configure properties such as QoS, NAT, schedules, and logging

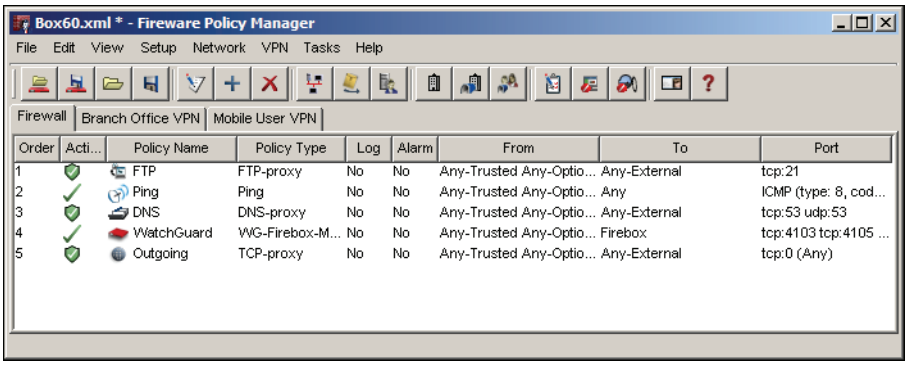
Changing the Policy Manager View

Policy Manager has two views: Large Icons and Details. The Large Icons view shows each policy as an icon. To change to the Large Icons view, select **Large Icons** from the **View** menu.



Large Icons View

To change to the Details view, select **Details** from the **View** menu. In the Details view, each policy is a row. You can see configuration information, including source and destination and logging and notification parameters.


Box60.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Firewall Branch Office VPN Mobile User VPN
Order Acti... Policy Name Policy Type Log Alarm From To Port
1 FTP FTP-proxy No No Any-Trusted Any-Optio... Any-External tcp:21
2 Ping Ping No No Any-Trusted Any-Optio... Any ICMP (type: 8, cod...
3 DNS DNS-proxy No No Any-Trusted Any-Optio... Any-External tcp:53 udp:53
4 WatchGuard WG-Firebox-M... No No Any-Trusted Any-Optio... Firebox tcp:4103 tcp:4105 ...
5 Outgoing TCP-proxy No No Any-Trusted Any-Optio... Any-External tcp:0 (Any)

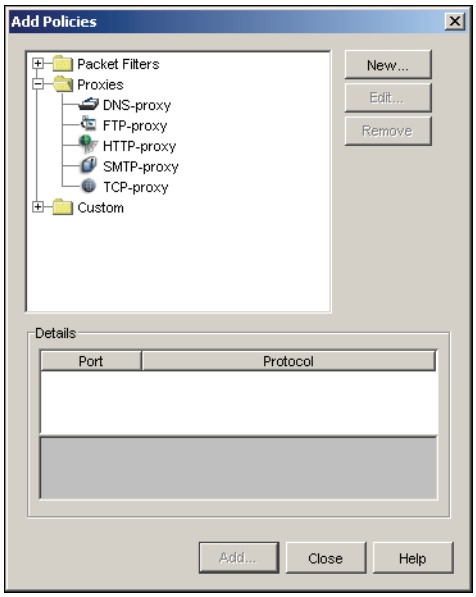
Details View

Adding a policy

You use Policy Manager to add a packet filter or proxy to your configuration. To add a policy:

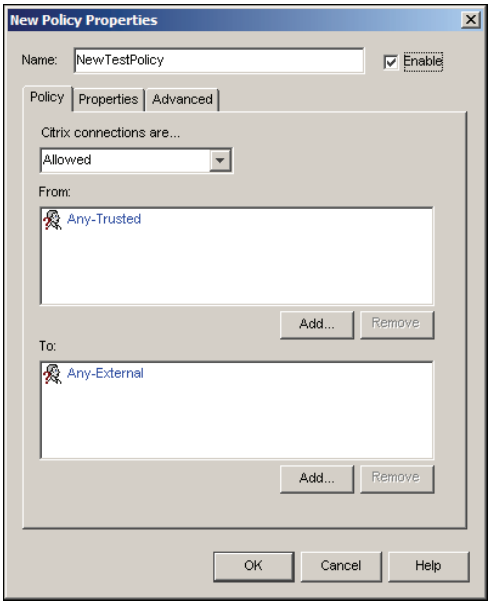
1 In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Policies dialog box appears.

2 Click the plus (+) sign on the left side of the folder to expand the **Packet Filters** or **Proxies** folders.
A list of packet filters or proxies appears.



3 Click the name of the policy to add.
When you select a policy, the policy icon appears in the area below the New, Edit, and Remove buttons. Also, the Details box shows the basic information about the policy.

4 Click **Add**.
The New Policy Properties dialog box appears.



5 You can change the name of the policy here. This information appears in the Policy Manager Details view. To change the name, type a new name in the **Name** text box.

6 Click **OK** to close the **Properties** dialog box.
You can add more than one policy while the Policies dialog box is open.

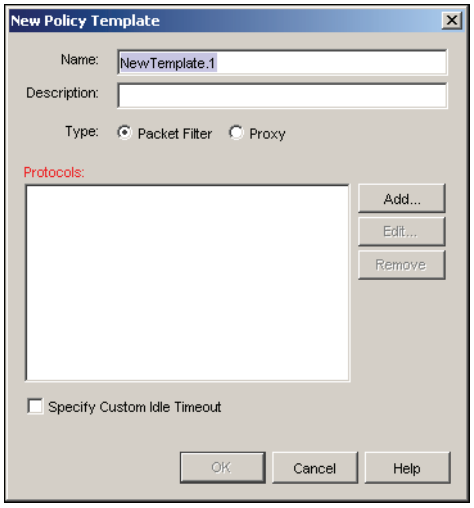
7 Click **Close**.
The new policy appears in Policy Manager. You can now set policy properties, as shown in "Configuring Policy Properties" on page 68.

Making a custom policy template

Policy Manager includes many packet filter policy templates. You can also make a custom policy template. A template includes ports and protocols that are unique to one type of network traffic. It could be necessary to make a custom policy template if you add a new software application behind your firewall.

1 In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Policies dialog box appears.

2 Click **New**.
The New Policy Template dialog box appears.

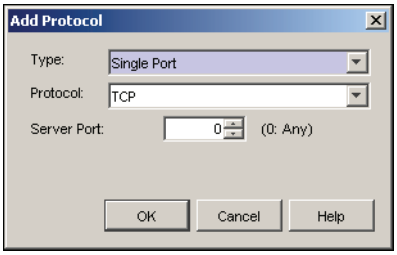


3 In the **Name** text box, type the name of the policy template.
This name must not be the same as names in the list in the Add Policy dialog box. The name appears in Policy Manager as the policy type. It helps you to find the policy when you want to change or remove it.

4 In the **Description** text box, type a description of the policy.
This appears in the Details section when you click the policy name in the list of User Filters.

5 Select the type of policy: **Packet Filter** or **Proxy**.
The Proxy option gives these options:
- DNS
- FTP
- HTTP
- TCP
- SMTP

6 To add protocols for this policy, click **Add**.
The Add Protocol dialog box appears.



7 From the **Type** drop-down list, select **Single Port** or **Port Range**.

8 From the **Protocol** drop-down list, select the protocol for this new policy. For more information about network protocols, see the *Reference Guide* or online help system. When you select **Single Port**, you can select:
- TCP
- UDP
- GRE
- AH

- ESP
- ICMP
- IGMP
- OSPF
- IP
- Any

When you select **Port Range**, you can select **TCP** or **UDP**.

9 From the **Server Port** drop-down list, select the port for this new policy. If you selected **Port Range**, select a starting server port and an ending server port.

10 Click **OK**.
Policy Manager adds the values to the New Policy Template dialog box. Make sure that the name, information, and configuration of this policy are correct. If necessary, click Add to configure more ports for this policy. Do the Add Port procedure again until you configure all ports for the policy.

11 Click **OK**.
The Add Policy dialog box appears with the new policy in the Custom folder.

Adding more than one policy of the same type

If your security policy lets you, you can add the same policy more than one time. For example, you can set a limit on the web access for most users, while you give full web access to your management. To do this, you make two different policies with different properties for outgoing traffic:

1 Add the first policy.

2 Change the name of the policy to give the function in your security policy and add the related information.
In this example, you can name the first policy "restricted_web_access."

3 Click **OK.** The **Properties** dialog box of the policy appears. Set the properties as shown in "Configuring Policy Properties" on page 68.

4 Add the second policy.

5 Click **OK.** The **Properties** dialog box of the policy appears. Set the properties.

Deleting a policy

As your security policy changes, you sometimes have to remove one or more policies. To remove a policy, you first remove it from Policy Manager. Then you save the new configuration to the Firebox.

1 From Policy Manager, click the policy.

2 In Policy Manager, click the **X** button on the Policy Manager toolbar.
You can also select Edit > Delete Policy.

3 When asked to confirm, click **Yes**.

4 Save the configuration to the Firebox and start the Firebox again. Select **File > Save > To Firebox**. Type the configuration passphrase. Select the **Save to Firebox** check box. Click **Save**.

Configuring Policy Properties

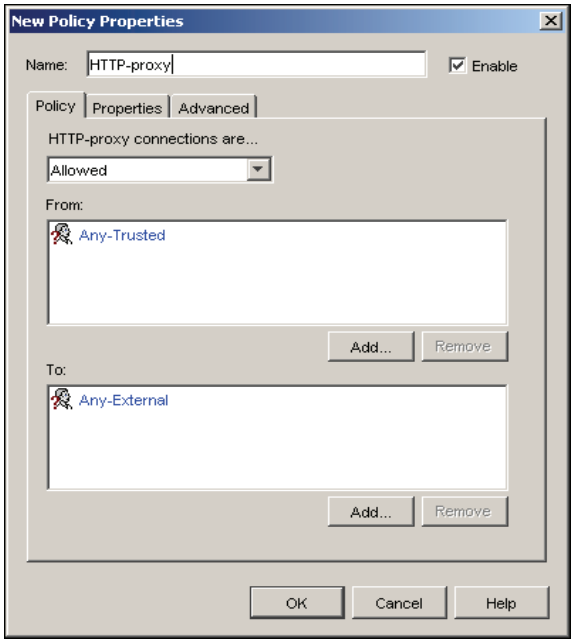
If you added a policy and want to change its properties, double-click the policy icon to open the **Edit Policy Properties** dialog box.

Setting access rules, sources, and destinations

You use the Policy tab to configure access rules for a given policy.

The **Policy** tab shows:

- If traffic that uses this policy is allowed or denied.
- Who uses this policy to start a connection with the users, hosts, and networks reachable through the Firebox®.
- The destinations for the traffic for this policy.



On the **From** list, you add the computers and networks that can send (or cannot send) network traffic with this policy. On the **To** list, you add computers and networks to which the Firebox routes traffic if it matches the policy specifications. For example, you could configure a ping packet filter to allow ping traffic from all computers on the external network to one web server on your optional network.

You can use these settings to configure how traffic is handled:

Allowed

The Firebox allows traffic that uses this policy if it obeys the rules you set in the policy.

Denied

The Firebox denies all traffic that matches this policy. You can configure it to record a log message when a computer tries to use this policy. It can also automatically add a computer or network that tries to start a connection with this policy to the Blocked Sites list (configured on the **Properties** tab).

Denied (send reset)

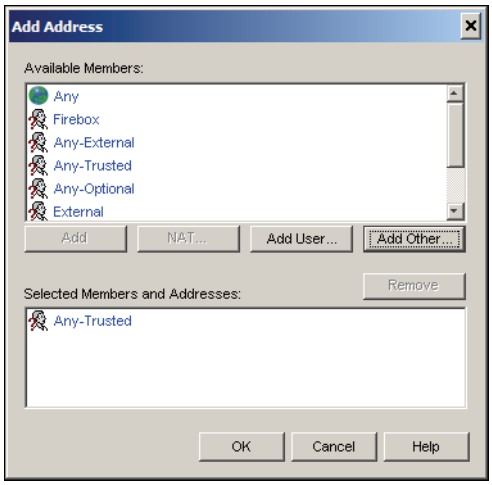
The Firebox denies all traffic that matches this policy. It can also automatically add a computer or network that tries to start a connection with this policy to the Blocked Sites list (configured on the **Properties** tab). The Firebox also sends a reset (RST) packet to tell the client that the session is refused and closed.

1 From the **Policy** tab, configure if connections are Allowed, Denied, or Denied (send reset).

2 To add members for the policy, click **Add** for the **From** or the **To** member list.

3 Use the **Add Address** dialog box to add a network, IP address, or specified user to a policy. Click either **Add User** or **Add Other.**

You can also select an item in the Available Members window and click **Add**, or double-click an item in this window. The Available Members list contains the aliases you add and the preconfigured aliases that Policy Manager gives.



4 If you selected **Add Other**, from the **Choose Type** drop-down list select the host range, host IP address, or network IP address to add. In the **Value** text box, type the correct network address, range, or IP address. Click **OK**.

The member or address appears in the Selected Members and Addresses list.

5 If you selected **Add User**, select the type of user or group, select the authentication server, and if you want to add a user or group.

Do this again to add other members and addresses. Your policy can have more than one object in the **From** or **To** field

6 Click **OK**.

Setting a proxy action

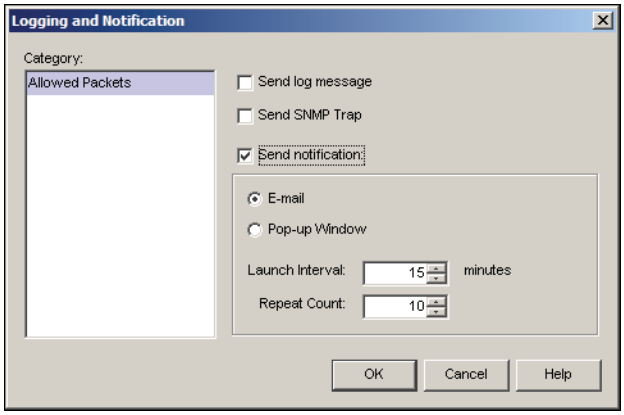
If you create a proxied policy, you can use the **Properties** tab of the **Policy Properties** dialog box to set a proxy action. For more information, see the "Configuring Proxied Policies" chapter.

This field is grayed out if you create a packet filter policy.

Setting logging properties

Use the **Properties** tab of the **Policy Properties** dialog box to set logging properties for a policy. You can configure the Firebox to record a log message when a policy denies packets. You can also set up notification when packets are allowed or denied.

1 From the **Properties** tab, click **Logging**.
The Logging and Notification dialog box appears.



2 Set the parameters and notification:

Enter it in the log

When you enable this check box, the Firebox sends a log message when it sees traffic of the type selected in the **Category** list. Domain name resolution on the Firebox can slow the time for the Firebox to send the log message to the log file. The default configuration of all policies is for the Firebox to send a log message when it denies a packet.

Send SNMP Trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The trap identifies the occurrence of a condition, such as a threshold that has exceeded its predetermined value.

Send notification

When you enable this check box, the Firebox sends a notification when it sees traffic of the type selected in the **Category** list. You set the notification parameters from the Log Server. For more information on the Log Server, refer to the *WatchGuard® System Manager Configuration Guide*. You can configure the Firebox to do one of these actions:

- **E-mail** The Firebox sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Firebox makes a dialog box appear on the management station when the event occurs.
  You can control the time of notification, together with the Repeat Count. For information how to use the Launch Interval and Repeat Count settings, see the next section.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, as follows:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents multiple notifications in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log entry about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are configured as:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 a.m. and continues each minute. This starts the logging and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

If the policy you configured is a proxy, a **Proxy** drop-down list appears with the View/Edit Proxy and Clone Proxy icons. For information on how to use these options, see the "Configuring Proxied Policies" chapter in this guide.

Note

One policy manages either allowed or denied traffic, but not both. If you want the Firebox to send log messages for both allowed and denied traffic, you must use different policies for each.

Configuring static NAT

Static NAT is also known as port forwarding. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a specified public address and port. Static NAT changes this address to an address and port behind the firewall. For more information on NAT, see the "Working with Firewall NAT" chapter in this guide.

Because of how static NAT operates, it is available only for policies that use a specified port, which includes TCP and UDP. A policy that uses a different protocol cannot use incoming static NAT. The **NAT** button in the **Properties** dialog box of that policy does not operate. You also cannot use Static NAT with the Any policy.

To help fight spam, many servers that receive e-mail do a reverse lookup of the source IP address the mail comes from. The receiving server does this to make sure that the sending server (the server sending the e-mail) is an authorized mail server for that domain. Because of this, we recommend that you assign your domain's MX (Mail eXchanger) DNS record IP address as the Firebox external IP address.

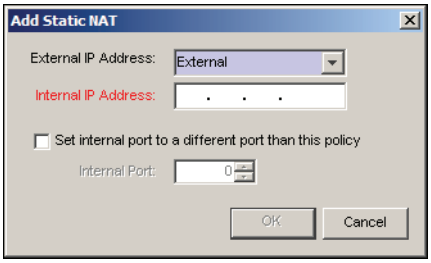
Usually, connections that start from a trusted or optional network and go to the Internet show the external IP address of the Firebox as the source IP address of the packets. If the Firebox external IP address is not your domain's MX record IP address, some remote servers will reject e-mail that you send. They do this because the SMTP session does not show your MX DNS record as the source IP address for the connection. If your Firebox does *not* use your MX record IP address as the external interface IP address, you can use a 1-to-1 NAT mapping to make outgoing e-mail connections show the correct source IP address. See the "Working with Firewall NAT" chapter for more information on 1-to-1 NAT.

1 In Policy Manager, double-click the policy icon.

2 From the **Connections are** drop-down list, select **Allowed**.
To use static NAT, the policy must let incoming traffic through.

3 Below the **To** list, click **Add**.
The Add Address dialog box appears.

4 Click **NAT**.
The Add Static NAT dialog box appears.



5 From the **External IP Address** drop-down list, select the "public" address to use for this policy.

6 Type the internal IP address.
The internal IP address is the destination on the trusted network.

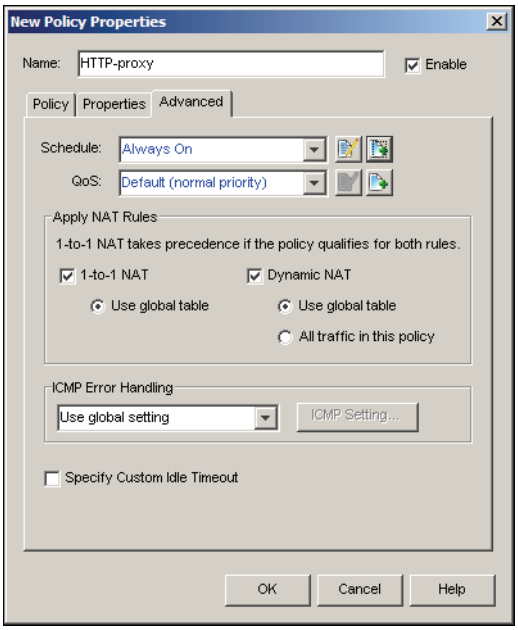
7 If necessary, select the **Set internal port to different port than service** check box.
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host, but also to a different port. If you select the check box, type the different port number or use the arrow buttons in the Internal Port box.

8 Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.

9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Properties** dialog box of the policy.

Setting advanced properties

You use the **Advanced** tab of the **Edit Policy Properties** dialog box to set the schedule, implement Quality of Service (QoS) settings, apply NAT rules, implement ICMP error handling for this policy, and implement a custom idle time-out.



Setting a schedule

You can set an operating schedule for the policy. You can use the schedule templates in the drop-down list or create a custom schedule. For information, see "Creating Schedules" on page 50.

Note that schedules can be shared by more than one policy.

Applying a Quality of Service (QoS) action

You can assign a Quality of Service action to the policy. Use the button on the far right to create a new QoS action. After you create a new QoS action, it appears in the **QoS** drop-down list. For more information, see "Creating QoS Actions" on page 186.

Note that these actions can be shared by more than one policy.

Applying NAT rules

You can apply Network Address Translation (NAT) rules to a policy:

1-to-1 NAT

With this type of NAT, the Firebox uses private and public IP ranges that you set, as described in "Using 1-to-1 NAT" on page 105.

Dynamic NAT

With this type of NAT, the Firebox maps private IP addresses to public IP addresses. Select **Use global table** if you want to use the dynamic NAT rules set for the Firebox. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

Setting ICMP error handling

You can set the ICMP error handling settings associated with the policy.

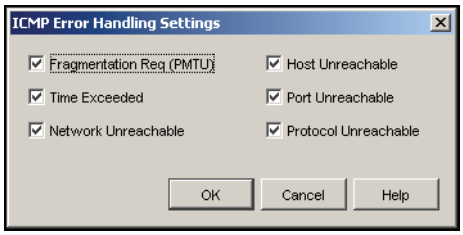
From the drop-down list, select:

Use global setting

Use the global ICMP error handling setting set for the Firebox. For information on this global setting, see "ICMP error handling" on page 40.

Specify setting

Configure a parameter that overrides the global setting. Click **ICMP Setting.** From the **ICMP Error Handling Settings** dialog box, select the check boxes to configure individual settings. For information on these settings, see "ICMP error handling" on page 40.



Setting a custom idle time-out

To set an idle time-out, click **Specify Custom Idle Timeout** and click the arrows to set the number of seconds before time-out. This setting overrides the idle time-out of the policy.

Setting Policy Precedence

Precedence is the sequence in which the Firebox® examines network traffic and applies a policy rule. The Firebox routes the traffic that uses the rules for the first policy that the traffic matches. Fireware™ Policy Manager automatically sorts policies from the most detailed to the most general. You can also manually set the precedence.

Using automatic order

Fireware Policy Manager automatically sorts policies from the most detailed to the most general. Each time you add a policy, Policy Manager compares the new rule with all the rules in your configuration file. To set the precedence, Policy Manager uses these criteria:

1 Protocols set for the policy type
2 Traffic rules of the **To** field
3 Traffic rules of the **From** field
4 Firewall action
5 Schedule
6 Alphanumeric sequence based on policy type
7 Alphanumeric sequence based on policy name

Comparing policy type

Policy Manager uses these criteria in sequence to compare two policies until it finds that the policies are equal or that one is more detailed than the other:

1 An Any policy always has the lowest precedence. For more information about the Any policy, see "Any" on page 227.

2 Check for the number of TCP 0 (any) or UDP 0 (any) protocols. The policy with the smaller number has higher precedence.

3 Check for the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.

4 Count the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.

5 Score the protocols based on their IP protocol value. The policy with the smaller score has higher precedence.

If Policy Manager cannot set the precedence when it compares the policy type, it examines traffic rules.

Comparing traffic rules

Policy Manager uses these criteria in sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy. It assigns higher precedence to the policy with the most detailed traffic rule. The list of traffic rules from most detailed to the most general:

1 Host address

2 IP address range (smaller than the subnet being compared to)

3 Subnet

4 IP address range (larger than the subnet being compared to)

5 Authentication user

6 Authentication group

7 Interface, Firebox

8 Any-External, Any-Trusted, Any-Optional

9 Any

For example, compare these two policies:

HTTP-1

From: Trusted, user1

HTTP-2

From: 10.0.0.1, Any-Trusted

"Trusted" is the most general entry for HTTP-1. "Any-Trusted" is the most general entry for HTTP-2. Because "Trusted" is within "Any-Trusted," HTTP-1 is the more detailed traffic rule. This is correct despite the fact that HTTP-2 includes an IP address.

If Policy Manager cannot set the precedence when it compares the traffic rules, it examines the firewall actions.

Comparing firewall actions

Policy Manager compares the firewall actions of two policies to set precedence. Precedence of firewall actions from highest to lowest is:

1 Denied or Denied (send reset)

2 Allowed Proxy

3 Allowed Filter

If Policy Manager cannot set the precedence when it compares the firewall actions, it examines the schedules.

Comparing schedules

Policy Manager compares the schedules of two policies to set precedence. Precedence of schedules from highest to lowest is:

1 Always off

2 Sometimes on

3 Always on

If the Policy Manager cannot set the precedence when it compares the schedules, it examines the policy names.

Comparing type and names

If the two policies do not match any other precedence criteria, Policy Manager sorts the policies in alphanumeric sequence. First it uses the policy type. Then it uses the policy name. Because no two policies can be the same type and have the same name, this is the last criteria for precedence.

Setting precedence manually

To switch to manual-order mode, select **View > Auto-order mode** so that the check disappears. You are asked to confirm if you want to switch to auto-order mode.

To change the order of policies:

- Select the policy whose order you want to change. Click the up or down arrow on the far right side of the Policy Manager toolbar.

or

- Select the policy whose order you want to change and drag it to its new location.

CHAPTER 7

Configuring Proxied Policies

Proxy filters do much more than packet filters. A proxy examines the contents of a packet, not only the header. As a result, the proxy finds forbidden content hidden or embedded in the data payload. For example, an SMTP proxy examines all incoming SMTP packets (e-mail) to find forbidden content, such as executable programs or files written in scripting languages. Attackers frequently use these methods to send computer viruses. The SMTP proxy knows these content types are not allowed, while a packet filter cannot detect the unauthorized content in the packet's data payload.

WatchGuard® proxies also look for application protocol anomalies and stop packets that are not made correctly. If an SMTP packet is not made correctly or contains unexpected content, it cannot go through the Firebox.

Proxy policies operate at the application, network, and transport protocol levels. Packet filter policies operate at only the network and transport protocol level. In other words, a proxy gets each packet, removes the network layer, and examines its payload. The proxy then puts the network information back on the packet and sends it to its destination on your trusted and optional networks. This adds more work for your firewall for the same volume of network traffic. But a proxy uses methods that packet filters cannot to catch dangerous packets.

Defining Rules

A ruleset is a group of rules based on one feature of a proxy. When you configure a proxy, you can see the rulesets for that proxy in the **Categories** list. The rulesets you see change when you change the proxy action on the **Properties** tab of a proxy configuration window.

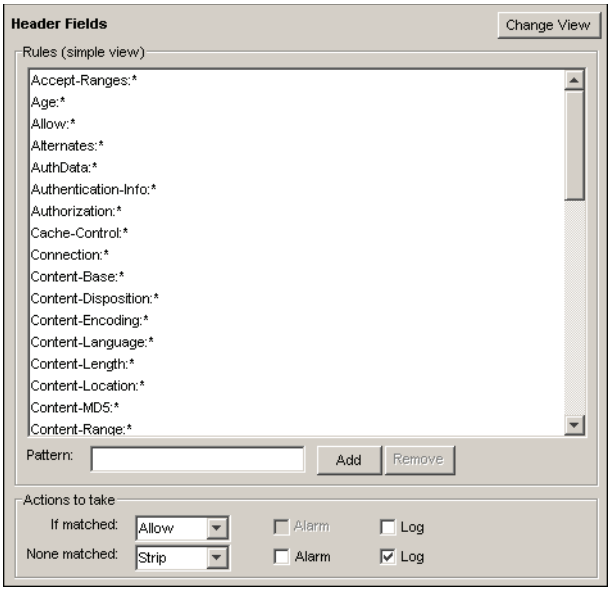
A proxy can have more than one proxy action associated with it. For example, you can use one ruleset for packets sent to an e-mail server protected by the Firebox® and a different ruleset to apply to e-mail messages being sent out through the Firebox to the Internet. You can use the existing proxy actions, or clone an existing proxy action to create a new proxy action.

A rule includes a type of content, pattern, or expression and the action the Firebox® does when a component of the packet's content matches a rule. Rules also include settings for when the Firebox sends alarms or if it sends events to the log file.

For most proxy features, the Firebox has a preinstalled ruleset. But you can edit the rules in a ruleset to change the action for the rules. You can also add your own rules.

The fields you use for these rule definitions look the same for each category of ruleset. The simple view is shown below. You can also select **Change View** to see the advanced view.

Use the advanced view to improve the matching function of a proxy. In advanced view, you can configure exact match and Perl-compatible regular expressions. In simple view, you can configure wildcard pattern matching with simple regular expressions.



Adding rulesets

From the simple view, do these steps to add new rules:

1 In the **Pattern** text box, type a pattern that uses simple regular expression syntax.
The wildcard for zero or more than one characters is "*".
The wildcard for one character is "?".

2 Click **Add**.
The new rule appears in the Rules box.

3 In the **Actions to take** section, the **If matched** drop-down list sets the action to occur if the contents of a packet match one of the rules in the list. The **None matched** drop-down list sets the action to occur if the contents of a packet do not match a rule in the list. Below is a list of all possible actions. The actions **Strip** and **Lock** apply only to signature-based intrusion prevention actions.

Allow
Allows the connection.

Deny
Denies a request but keeps the connection if possible.

Drop
Denies the specific request and drops the connection.

Block
Denies the request, drops the connection, and adds the source host to the Blocked Sites list. For more information on blocked sites, see "Setting Blocked Sites" on page 135.

Strip

Removes an attachment from a packet and discards it. The other parts of the packet are sent through the Firebox to its destination.

Lock

Locks an attachment, and wraps it so that it cannot be opened by the user. Only the administrator can unlock the file.

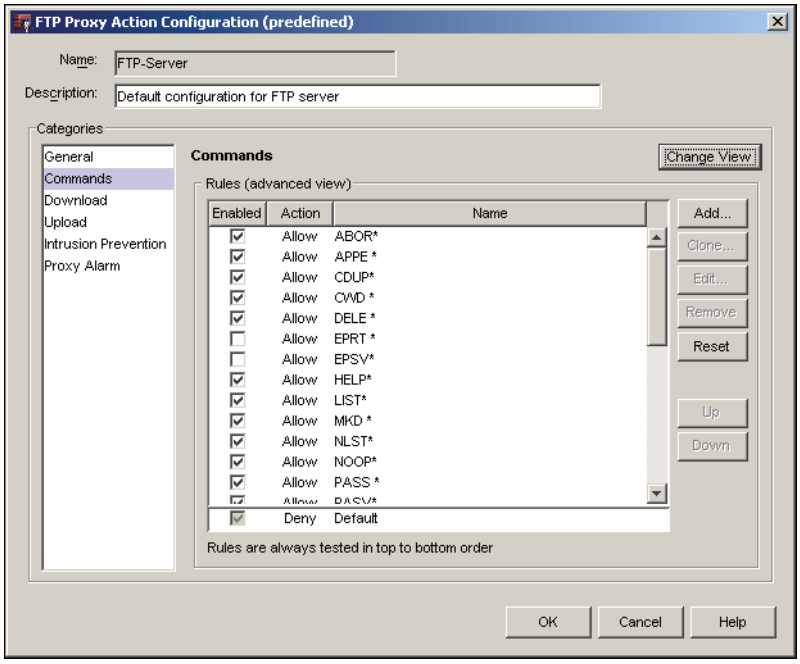
4 An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box to configure an alarm for this event. To set the options for the alarm, select **Proxy Alarm** from the **Categories** list on the left side of a Proxy Configuration window. You can send an SNMP trap, send e-mail, or open a pop-up window.

5 Use the **Log** check box to write a traffic log message for this event.

Using advanced rules view

To see a detailed view of the current rules, click **Change View**. The advanced view shows the action for each rule. It also has buttons you can use to edit, clone (use an existing rule definition to start a new one), delete, or reset rules. To go back to the simple view, click **Change View** again.

The main advantage of the advanced view is that you can set allowed and denied rules in the same ruleset. You cannot go back to simple view if the enabled rules have different action, alarm, and log settings. In this case, you must continue to use the advanced view.



Changing the precedence of rules

The Firebox uses these guidelines to apply rules:

- It applies the rules in sequence from the top to the bottom of the window.
- When a filtered item matches a rule, the Firebox applies the related traffic action.
- Content can match more than one of the rules or the default rule, but only the first rule is used.

- The Firebox uses the default rule if no other rule applies. It is always the last rule that the Firebox applies to the content.

To change the sequence of rules, you must use the advanced view:

1 Click **Change View** to see the advanced view of created rules.

2 Select a rule to move up or down in the list. Click the **Up** or **Down** button to move the rule up or down in the list.

Customizing Logging and Notification for Proxy Rules

An alarm, log message, or notification is a mechanism to tell a network administrator about network traffic that does not match the criteria for allowed traffic. For example, if traffic is more than a threshold value, you can configure the Firebox® to send you an e-mail message. You can set alarm, log message, and notification properties for each packet filter and proxy policy. You can also set alarm and log message properties for a proxy rule.

Configuring log messages and notification for a proxy policy

1 Double-click the policy icon to open the **Policy Properties** dialog box.

2 Click the **Properties** tab. Click **Logging**.
The Logging and Notification dialog box appears.

3 Set the parameters to match the requirements of your security policy.

Configuring log messages and alarms for a proxy rule

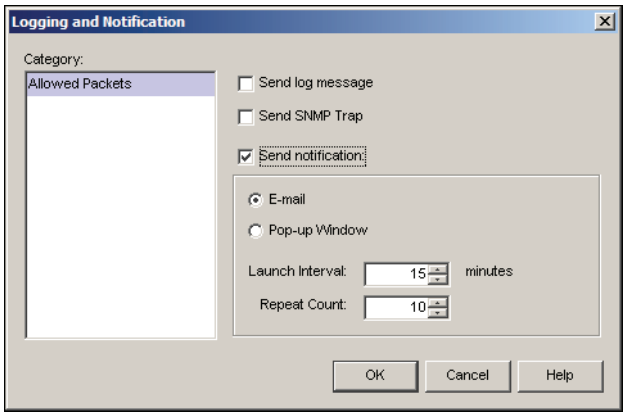
1 Double-click the policy icon to open the **Policy Properties** dialog box.

2 Click the **Properties** tab. From the **Proxy** drop-down list, select the proxy action to configure.

3 Select **Proxy Alarms** from the **Category** list. For more information about the parameters, see the subsequent section.
There are more log messages and notification options available with signature-based intrusion prevention services. These options are examined in the chapter "Using Signature-Based Security Services."

Using dialog boxes for alarms, log messages, and notification

The dialog boxes for alarms, log messages, and notification in proxy definitions have most or all of these fields:



Enter it in the log

When you enable this check box, the Firebox sends a traffic log message to the Log Server when this event occurs. The default configuration of all policies is for the Firebox to send a log message when it denies a packet.

Send SNMP Trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The SNMP trap shows when the traffic matches a condition such as a property that is more than its threshold value. Note that the bindings section in the SNMP trap is blank if the trap occurs when SNMP starts or stops, such as with a reset, restart, or failover.

Send notification

When you enable this check box, the Log Server sends a notification when this event occurs. You can configure the Log Server to do one of these actions:

- **E-mail** The Log Server sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Log Server makes a dialog box appear on the management station when the event occurs.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, with these parameters:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log message about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are set up as follows:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 AM and continues each minute. This starts the log and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

Configuring the SMTP Proxy

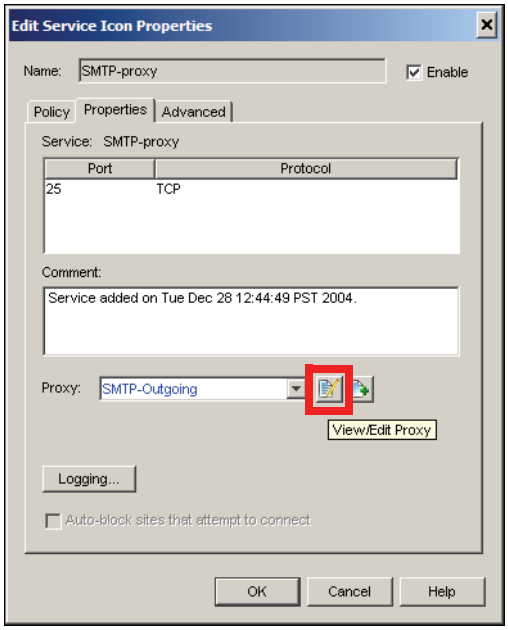
You use the SMTP proxy to block suspicious e-mail messages and e-mail content. The proxy scans SMTP messages for a number of filtered parameters, and compares them against the rules set in the proxy configuration. To configure the SMTP proxy:

1 Add the SMTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 64.

2 Double-click the SMTP icon and select the **Properties** tab.
The Edit Policy Properties dialog box appears and shows the General Settings information.

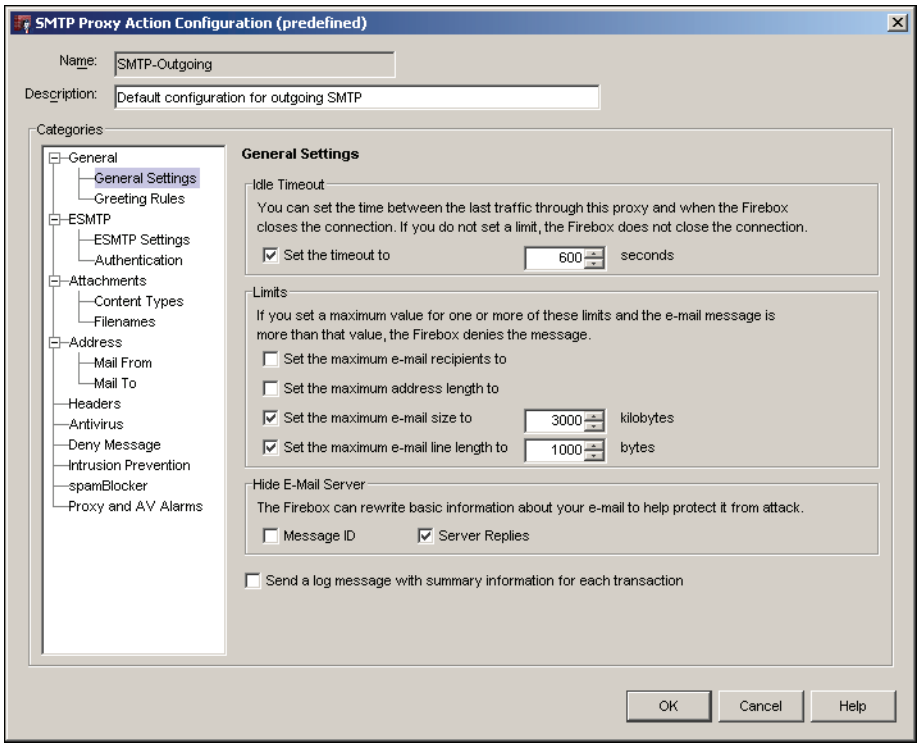
3 In the **Proxy** drop-down list, select to configure SMTP-Incoming or SMTP-Outgoing.
You can also clone a proxy action to create a new proxy action.

4 Click the **View/Edit Proxy** icon.



Configuring general settings

You use the **General Settings** fields to configure basic SMTP proxy parameters, including idle time-out and message limits.



Idle timeout

You can set the length of time an incoming SMTP connection can stay idle before the connection is closed. The default value is 600 seconds (10 minutes). For no time-out, clear the **Set the timeout to** check box.

Maximum e-mail recipients

With the **Set the maximum e-mail recipients to** check box, you can set the maximum number of e-mail recipients to which a message can be sent. The Firebox® counts and allows the specified number of addresses through, then drops the other addresses. For example, if you use the default value of 50 and there is a message for 52 addresses, the first 50 addresses get the e-mail message. The last two addresses do not get a copy of the message. A distribution list appears as one SMTP e-mail address (for example, support@watchguard.com). The Firebox counts this as one address.

You can use this feature to decrease spam e-mail because spam usually includes a large recipient list. Be careful when you do this because you can also deny legitimate e-mail.

Maximum address length

With the **Set the maximum address length to** check box, you can set the maximum length of e-mail addresses.

Maximum e-mail size

With the **Set the maximum e-mail size to** check box, you can set the maximum length of an incoming SMTP message. Most e-mail is sent as 7-bit ASCII text. The exceptions are Binary MIME and 8-bit MIME. 8-bit MIME content (for example, MIME attachments) is encoded with standard algorithms (Base64 or quote-printable encoding) to enable them to be sent through 7-bit e-

mail systems. Encoding can increase the length of files by as much as one third. To allow messages as large as 1000 bytes, you must set this field to a minimum of 1334 bytes to make sure all e-mail gets through. The default value is 3,000,000 bytes (3 million bytes).

Maximum e-mail line length

With the **Set the maximum e-mail line length to** check box, you can set the maximum line length for lines in an SMTP message. Very long line lengths can cause buffer overflows on some e-mail systems. Most e-mail clients and systems send short line lengths, but some web-based e-mail systems send very long lines. The default value is 1024.

Hide E-mail Server

Select the **Message ID** and **Server Replies** check boxes to replace MIME boundary and SMTP greeting strings in e-mail messages. These are used by hackers to identify the SMTP server vendor and version.

Send a log message

Select the **Send a log message** check box to send a log message for each connection request through SMTP. For Historical Reports to create accurate reports on SMTP traffic, you must select this check box.

Greeting rules

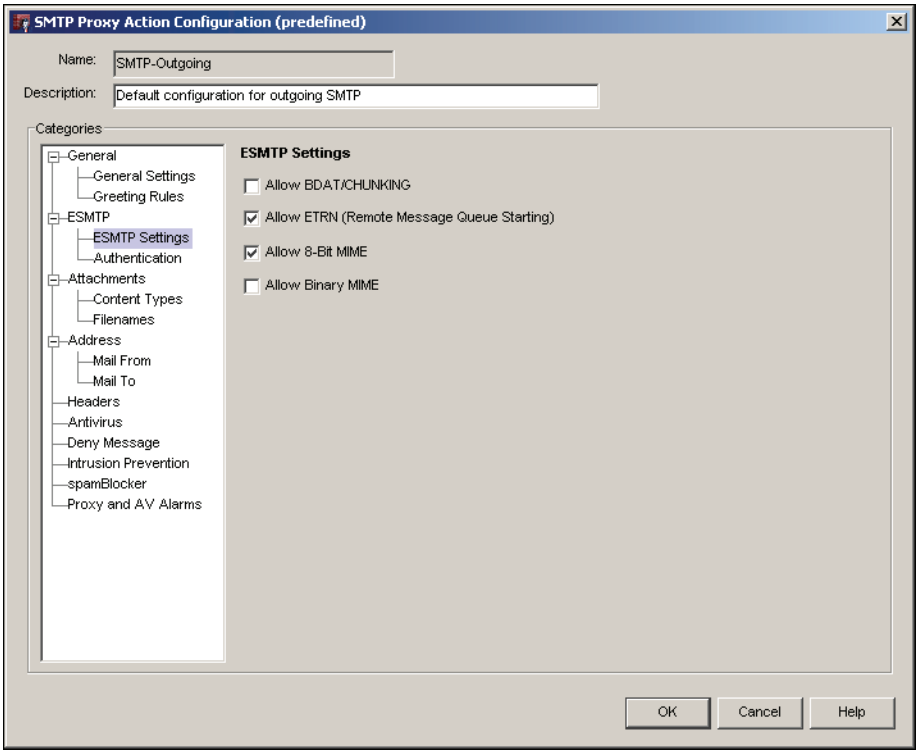
The proxy examines the initial HELO/EHLO responses during the SMTP session initialization. The default rules for the SMTP-Incoming proxy action make sure that packets with greetings that are too long, or include characters that are not correct or expected, are denied.

Configuring ESMTP parameters

You use the **ESMTP Settings** fields to set the rules for ESMTP content filtering. Although SMTP is widely accepted and widely used, some parts of the Internet community have found a need to extend SMTP to

allow more functionality. ESMTP gives a method for functional extensions to SMTP, and for clients who support extended features to know each other.

1 From the **Categories** section, select **ESMTP Settings**.



Allow BDAT/CHUNKING

Select to allow BDAT/CHUNKING. This enable large messages to be sent more easily through SMTP connections.

Allow ETRN (Remote Message Queue Starting)

This is an extension to SMTP that allows an SMTP client and server to interact to start the exchange of message queues for a given host.

Allow 8-Bit MIME

Select to allow 8-bit MIME, if the client and host give support to the extension. The 8-bit MIME extension allows a client and host to exchange messages made up of text that has octets which are not of the US-ASCII octet range (hex 00-7F, or 7-bit ASCII) that uses SMTP.

Allow Binary MIME

Select to allow the Binary MIME extension, if the sender and receiver accept it. Binary MIME prevents the overhead of base64 and quoted-printable encoding of binary objects sent that use the MIME message format with SMTP. WatchGuard does not recommend you select this option as it can be a security risk.

Configuring authentication rules

This ruleset allows a number of ESMTP authentication types. The default rule denies all other authentication types. The RFC that tells about the SMTP authentication extension is RFC 2554.

1 From the **Categories** section, select **Authentication**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Defining content type rules

You use the ruleset for the SMTP-Incoming proxy action to set values for incoming SMTP content filtering. You use the ruleset for the SMTP-Outgoing proxy action to set values for outgoing SMTP content filtering.

1 From the **Categories** section, select **Content Types**.

2 Do the steps used to create rules. For more information, see "Defining Rulesets" on page 79.

Defining file name rules

You use the ruleset for the SMTP-Incoming proxy action to put limits on file names for incoming e-mail attachments. You use the ruleset for the SMTP-Outgoing proxy action to put limits on file names for outgoing e-mail attachments.

1 From the **Categories** section, select **Filenames**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Configuring the Mail From and Mail To rules

The **Mail From** ruleset can put limits on e-mail to only allow e-mail into your network from specified senders. The default configuration is to allow e-mail from all senders.

The **Mail To** ruleset can put limits on e-mail to only allow e-mail out of your network to specified recipients. The default configuration allows e-mail to a recipient out of your network.

You can also use the **Rewrite As** feature included in this rule configuration dialog box to have the Firebox change the From and To components of your e-mail address to a different value. This feature is also known as "SMTP masquerading."

1 From the **Categories** section, select **Mail From** or **Mail To**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Defining header rules

Header rulesets allow you to set values for incoming or outgoing SMTP header filtering.

1 From the **Categories** section, select **Headers**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Defining antivirus responses

The fields on this dialog box set the actions to occur if a virus is found in an e-mail message. It also sets actions for when an e-mail message contains an attachment that is too large or that the Firebox cannot scan.

Although you can use the proxy definition screens to activate and configure Gateway AntiVirus, it is easier to use **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the antivirus screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Changing the deny message

The Firebox® gives a default deny message that replaces the denied content. You can replace that deny message with one that you write. You can write a custom deny message with standard HTML. The first line of the deny message is a section of the HTTP header. There must be an empty line between the first line and the body of the message.

1 From the **Categories** section, select **Deny Message**.

2 Type the deny message in the deny message box. You can use these variables:

%(reason)%
Puts the cause for the Firebox to deny the content.

%(type)%
Puts the type of content that was denied.

%(filename)%
Puts the file name of the denied content.

%(virus)%
Puts the name or status of a virus, for Gateway AntiVirus users only.

%(action)%
Puts the name of the action taken: lock, strip, and so on.

%(recovery)%
Allows you to set the text to fill this sentence: "Your network administrator %(recovery)% this attachment.

Configuring the IPS (Intrusion Prevention System) for SMTP

Hackers use many methods to attack computers on the Internet. The function of these attacks is to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as *intrusions*.

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Configuring spamBlocker

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard® spamBlocker™ option increases your capacity to catch spam at the edge of your network when it tries to come into your system.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the spamBlocker screens in the proxy definition, see the chapter "Using spamBlocker."

Configuring proxy and antivirus alarms for SMTP

You can set the action the Firebox does when proxy or antivirus (AV) alarm events occur:

1 From the **Categories** section, select **Proxy and AV Alarms.**

2 For information on fields in the **Proxy/AV Alarm Configuration** section, see "Using dialog boxes for alarms, log messages, and notification" on page 83.

Configuring the FTP Proxy

File Transfer Protocol (FTP) is the protocol used to move files on the Internet. Like SMTP and HTTP, FTP uses TCP/IP protocols to enable data transfer. You usually use FTP to download a file from a server that uses the Internet or to upload a file to a server.

1 Add the FTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 64.

2 Double-click the FTP icon and select the **Policy** tab.

3 Select **Allowed** from the **FTP proxy connections are** drop-down list.

4 Select the **Properties** tab.

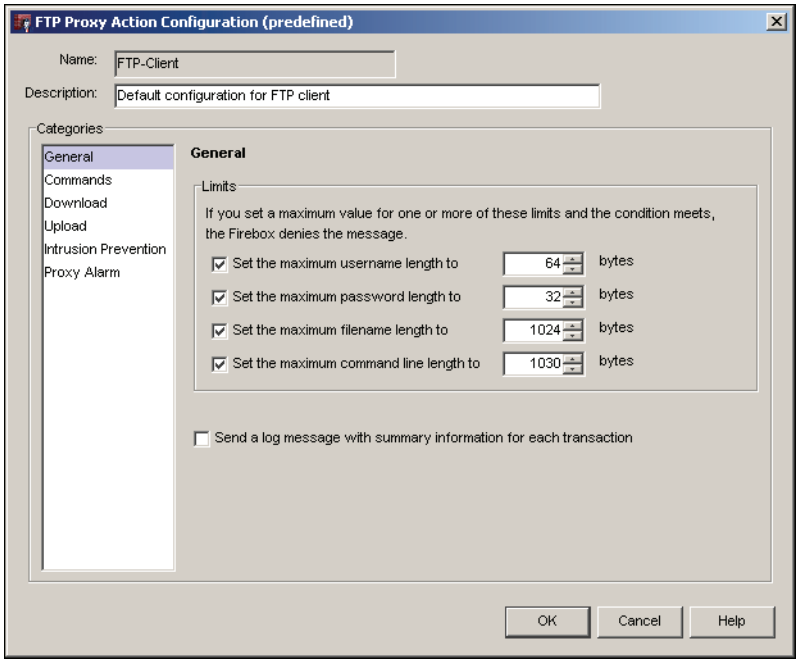
5 In the **Proxy** drop-down list, select to configure the proxy action for FTP-Client or FTP-Server.

6 Click the **View/Edit Proxy** icon.

Configuring general settings

You use the **General** fields to configure basic FTP parameters including maximum user name length.

1 From the **Categories** section, select **General.**



2 To set limits for FTP parameters, select the applicable check boxes. These settings help to protect your network from buffer overflow attacks. If you set a check box to 0 bytes, the Firebox does not use the parameter. Use the arrows to set the limits:

Maximum user name length
Sets a maximum length for user names on FTP sites.

Maximum password length
Sets a maximum length for passwords used to log in to FTP sites.

Maximum file name length
Sets the maximum file name length for files to upload or download.

Maximum command line length
Sets the maximum length for command lines used on FTP sites.

3 To create a log message for each transaction, select the **Send a log message with summary information for each transaction** check box.

Defining commands rules for FTP

FTP has a number of commands to manage files. You can write rules to put limits on some FTP commands. Use FTP-Server to put limits on commands that can be used on an FTP server protected by the Firebox. Use FTP-Client to put limits on commands that users protected by the Firebox can use when it connects to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

1 From the **Categories** section, select **Commands.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting download rules for FTP

Download rules control the file names, extensions, or URL paths that users can use FTP to download. Use the FTP-Server proxy action to control download rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set download rules for users connecting to external FTP servers. To add download rulesets:

1 From the **Categories** section, select **Download.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting upload rules for FTP

Upload rulesets control the file names, extensions, or URL paths that users can use FTP to upload. Use the FTP-Server proxy action to control upload rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set upload rules for users connecting to external FTP servers. The default configuration of the FTP-Client is to allow all files to be uploaded. To create upload rulesets:

1 From the **Categories** section, select **Upload.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Enabling intrusion prevention for FTP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

.Configuring proxy alarms for FTP

An alarm is a mechanism to tell a network administrator when network traffic matches criteria for suspicious traffic or content. When an alarm event occurs, the Firebox® does an action that you configure. For example, you can set a threshold value for file length. If the file is larger than the threshold value, the Firebox can send a log message to the Log Server.

1 From the **Categories** section, select **Proxy Alarm.**

2 For information on fields in the **Proxy Alarm Configuration** section, see "Using dialog boxes for alarms, log messages, and notification" on page 83.

Configuring the HTTP Proxy

The HTTP proxy is a high performance content filter. It examines web traffic to identify suspicious content that could be a virus, spyware, or other type of attack. It can also protect your web server from attacks from the external network. You can configure the HTTP proxy to:

- Only allow content that matches RFC requirements for web server and clients
- Select which types of MIME content the Firebox® allows into your network
- Block Java, ActiveX, and other code types
- Examine the HTTP header to make sure it is not from a known source of suspicious content

1 Add the HTTP proxy to Policy Manager. To learn how to add policies to Policy Manager, see"Adding Policies" on page 64.

2 Select the **Properties** tab.

3 In the **Proxy** drop-down list, select to configure the HTTP-Client or HTTP-Server proxy action. Use the HTTP-Server proxy action (or an incoming proxy action you create based on the HTTP-Server proxy action) to protect a web server. Use HTTP-Client, or an outgoing proxy action, to filter HTTP requests from users behind the Firebox.

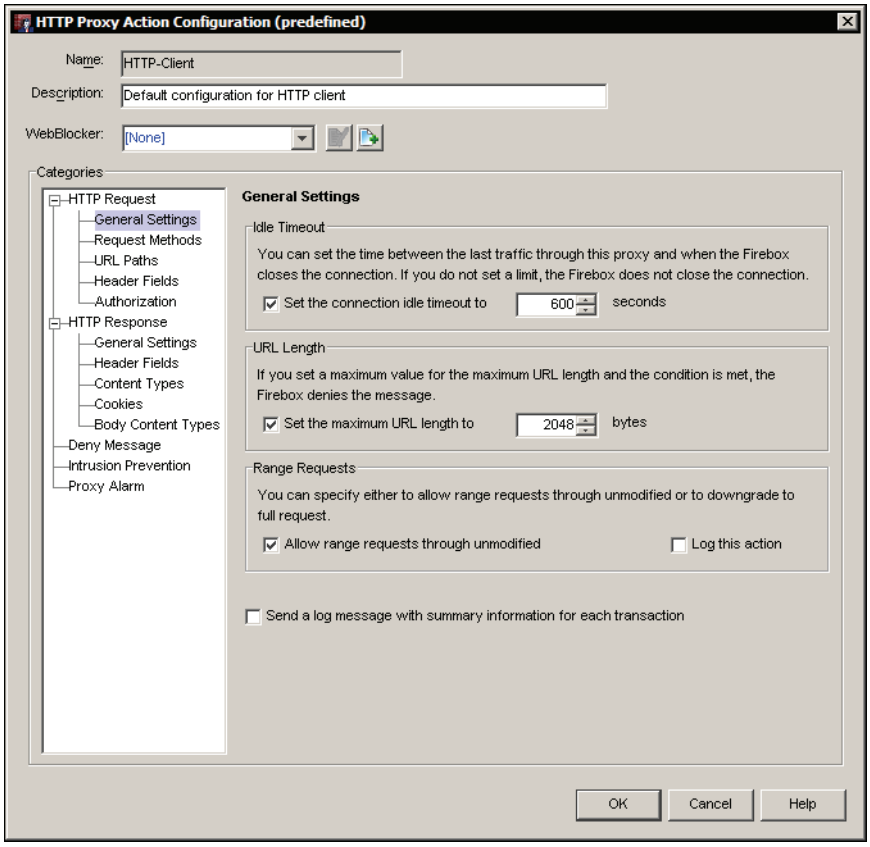
4 Click the **View/Edit Proxy** icon.
You can also clone a proxy action to create a new proxy action.

Configuring settings for HTTP requests

You can configure general settings for HTTP requests. You can also see and edit the HTTP request rulesets included in a proxy action. To get access to these settings, click **HTTP Request** in the **Categories** list on the left of the proxy configuration.

Configuring general settings for HTTP requests

You use the **General Settings** fields to configure basic HTTP parameters such as idle time-out and URL length.



Idle Timeout

Controls how long the HTTP proxy waits for the web client to make a request for something from the external web server after it starts a TCP/IP connection or after the earlier request, if there was one, for the same connection. If it goes longer than the setting, the HTTP proxy closes the connection. The default value is 600 seconds.

URL Length

Sets the maximum length of the path component of an URL. This does not include the "http:\\" or host name. Control of the URL length can help to prevent buffer overflow attacks.

Range requests

Range requests allow a client to request subsets of the bytes in a web resource instead of the full content. For example, this is useful when you want only some sections of a large Adobe file. You can select a range request to prevent the download of unnecessary pages.

Send a log message with summary information for each transaction

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked.

Setting HTTP request methods

Most browser HTTP requests are in one of two categories: GET and POST operations. Browsers usually use GET operations to download objects such as a graphic, HTML data, or Flash data. More than one GET is usually sent by a client computer for each page, because web pages usually contain many different elements. The elements are put together to make a page that appears as one page to the end user.

Browsers usually use POST operations to send data to a web site. Many web pages get information from the end user such as location, e-mail address, and name. If you enable the POST command, the Firebox denies all POST operations to web servers on the external network. This features prevents your users from sending information to a web site on the external network.

The HTTP proxy supports request methods: HEAD, GET, POST, OPTIONS, PUT, and DELETE. If you configure a rule to allow other request methods, you get an error with the text: "Method unsupported."

1 From the **Categories** section, select **Request Methods**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request URL paths

You use URL path rules to filter the content of the host, path, and query-string components of a URL. Here are examples of how to block content using HTTP request URL paths:

- To block all pages that have the host name www.test.com, type the pattern: www.test.com*
- To block all paths that contain the word "sex", on all web sites: *sex*
- To block URL paths that end in "*.test", on all web sites: *.test

Note

Usually, if you filter URLs with the HTTP request URL path ruleset, you must configure a complex pattern using full regular expression syntax and the advanced view of a ruleset. It is easier and gives better results to filter based on header or body content type than it is to filter by URL path.

1 From the **Categories** section, select **URL paths**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request header fields

This ruleset supplies content filtering for the full HTTP header. By default, the Firebox uses exact matching rules to strip Via and From headers, and allows all other headers. This ruleset matches against the full header, not only the name. Thus, to match all values of a header, type the pattern: "[*header name*]:*". To match only some values of a header, replace the * wildcard with a pattern. If your pattern does not start with a * wildcard, include one space between the colon and the pattern when typing in the **Pattern** text box. For example, type: [*header name*]: [*pattern*] and not [*header name*]:[*pattern*].

Note that the default rules do not strip the Referer header, but do include a disabled rule to strip this header. To enable the rule, select **Change View**. Some web browsers and software applications must use the Referer header to operate correctly.

1 From the **Categories** section, select **Header Fields**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP request authorization

This rule sets the criteria for content filtering of HTTP Request Header authorization fields. When a web server starts a "WWW-Authenticate" challenge, it sends information about which authentication methods it can use. The proxy puts limits on the type of authentication sent in a request. It uses only the

authentication methods that the web server accepts. With a default configuration, the Firebox allows Basic, Digest, NTLM, and Passport1.4 authentication, and strips all other authentication.

1 From the **Categories** section, select **Authorization**.

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Configuring general settings for HTTP responses

You use the General Settings fields to configure basic HTTP parameters such as idle time-out and limits for line and total length. If you set a check box to zero bytes, the Firebox does not check the parameter.

1 From the **Categories** section, select **General Settings**.

2 To set limits for HTTP parameters, select the applicable check boxes. Use the arrows to set the limits:

Idle timeout
: Controls how long the Firebox HTTP proxy waits for the web server to send the web page. The default value is 600 seconds.

Maximum line length
: Controls the maximum allowed length of a line of characters in the HTTP response headers. Use this property to protect your computers from buffer overflow exploits.

Maximum total length
: Controls the maximum length of the HTTP response headers. If the total header length is more than this limit, the HTTP response is denied. The default value is 0 (no limit).

Setting header fields for HTTP responses

This property controls which HTTP response header fields the Firebox allows. RFC 2616 includes many of the HTTP response headers that are allowed in the default configuration. For more information, see:

http://www.ietf.org/rfc/rfc2616.txt

1 From the **Categories** section, select **Header Fields.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting content types for HTTP responses

When a web server sends HTTP traffic, it usually adds a MIME type to the response. The HTTP header on the data stream contains this MIME type. It is added before the data is sent.

This ruleset sets rules for looking for content type (MIME type) in HTTP response headers. By default the Firebox allows some safe content types, and denies MIME content that has no specified content type. Some web servers supply incorrect MIME types to bypass content rules.

1 From the **Categories** section, select **Content Types.**

2 Do the steps used to create rulesets. For more information, see "Defining Rules" on page 79.

Setting cookies for HTTP responses

HTTP cookies are small files of alphanumeric text put by web servers on web clients. Cookies monitor the page a web client is on to enable the web server to send more pages in the correct sequence. Web servers also use cookies to collect information about an end user. Many web sites use cookies for authentication and other legitimate functions and cannot operate correctly without cookies.

This ruleset gives you control of the cookies in HTTP responses. You can configure rules to strip cookies, based on your network requirements. The default rule for the HTTP-Server and HTTP-Client proxy action allows all cookies.

The Cookies ruleset looks for packets based on the domain associated with the cookie. The domain can be specified in the cookie. If there is no domain in the cookie, the proxy uses the host name in the first request. Thus, to block all cookies for nosy-adware-site.com, add a rule with the pattern: "*.nosy-adware-site.com".

1 From the **Categories** section on the left, select **Cookies.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Setting HTTP body content types

This ruleset gives you control of the content in an HTTP response. The Firebox is configured to deny Java applets, Zip archives, Windows EXE/DLL files, and Windows CAB files. The default proxy action for outgoing HTTP requests (HTTP-Client) allows all other response body content types. WatchGuard recommends that you examine the file types that are used in your organization and allow only those file types that are necessary for your network.

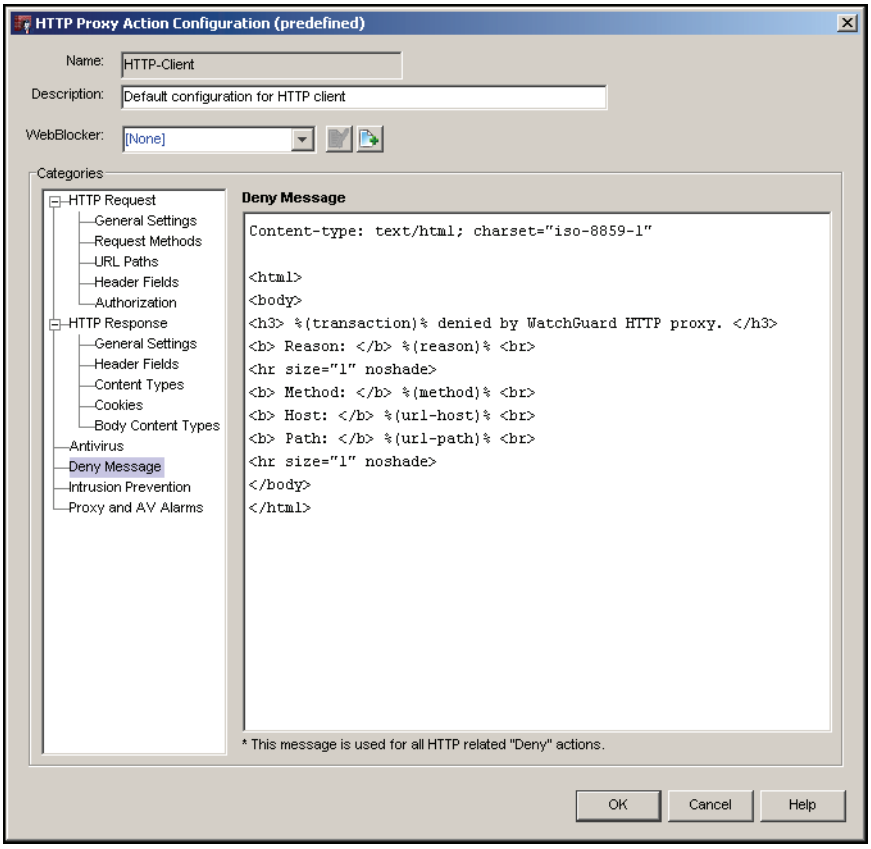
1 From the **Categories** section, select **Body Content Types.**

2 Do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Changing the deny message

The Firebox gives a default deny message that replaces the content that is denied. You can replace that deny message with one that you write. You can customize the deny message with standard HTML. The first line of the deny message is a component of the HTTP header. There must be an empty line between the first line and the body of the message.

1 From the **Categories** section, select **Deny Message**.



2 Type the deny message in the deny message box. You can use these variables:

%(transaction)%
Puts "Request" or "Response" to show which side of the transaction caused the packet to be denied.

%(reason)%
Puts the reason the Firebox denied the content.

%(method)%
Puts the request method from the denied request.

%(url-host)%
Puts the server host name from the denied URL. If no host name was included, the IP address of the server is given.

%(url-path)%
Puts the path component of the denied URL.

Enabling intrusion prevention for HTTP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Defining proxy and antivirus alarms for HTTP

Use these settings to set criteria for a notification event:

1 From the **Categories** section, select **Proxy and AV Alarms.**

2 Do the steps in "Using dialog boxes for alarms, log messages, and notification" on page 83.

Configuring the DNS Proxy

With the Domain Name System (DNS), you can get access to a web site with an easy-to-remember "dot-com" name. DNS finds the Internet domain name (for example WatchGuard.com) and changes it to an IP address. The DNS proxy protects your DNS servers from TSIG, NXT, and other DNS attacks. To add the DNS proxy to your Firebox® configuration:

1 Add the DNS proxy to Policy Manager. To learn how to add policies to Policy Manager, see "Adding Policies" on page 64.

2 Double-click the DNS icon and select the **Policy** tab.

3 Select **Allowed** from the **DNS proxy connections are** drop-down list.

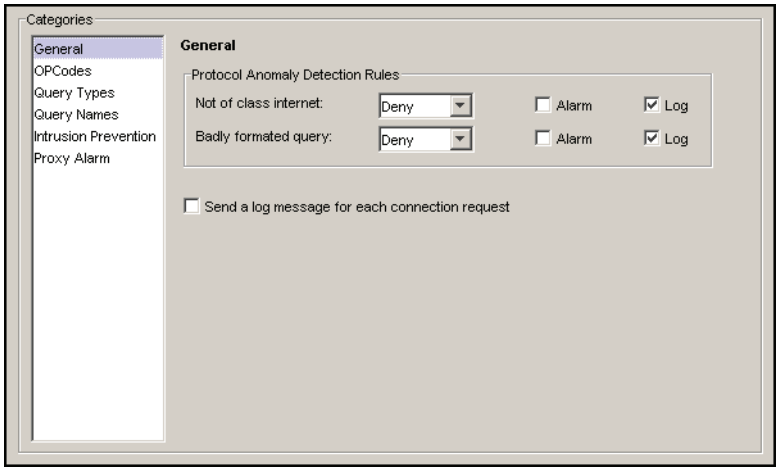
4 Select the **Properties** tab.

5 In the **Proxy** drop-down list, select to configure the NS-Outgoing or DNS-Incoming proxy action.

6 Click the **View/Edit Proxy** icon.
You can also clone an existing proxy action to create a new proxy action.

Configuring general settings for the DNS proxy

The general settings for the DNS Proxy include two protocol anomaly detection rules



Not of class Internet

Select the action to do when the proxy examines DNS traffic that is not of the Internet (IN) class. The default action is to deny this traffic. We recommend that you do not change this default action. Use the **Alarm** check box to use an alarm for this event. Use the **Log** check box to record this event in the log file.

Badly formatted query

Select the action when the proxy examines DNS traffic that does not use the correct format. Use the **Alarm** check box to use an alarm for this event. Use the **Log check box** to record this event in the event log file.

Send a log message with summary information for each transaction

Select this check box to record a log message for each DNS connection request. Note that this creates a large number of log messages and more traffic.

Configuring DNS OPcodes

DNS OPcodes are commands given to the DNS server that tell it to do some action, such as a query (Query), an inverse query (IQuery), or a server status request (STATUS). You can allow, deny, drop, or block specified DNS OPcodes.

1 From the **Categories** section, select **OPCodes**.

2 For the rules listed, select the **Enabled** check box to enable a rule. Clear the **Enabled** check box to disable a rule.

Note

If you use Active Directory and your Active Directory configuration requires dynamic updates, you must allow DNS OPcodes in your DNS-Incoming proxy action rules. This is a security risk, but can be necessary for Active Directory to operate correctly.

Adding a new OPcodes rule

1 Click **Add**.
The New OPCodes Rule dialog box appears.

2 Type a name for the rule.
Rules can have no more than 31 characters.

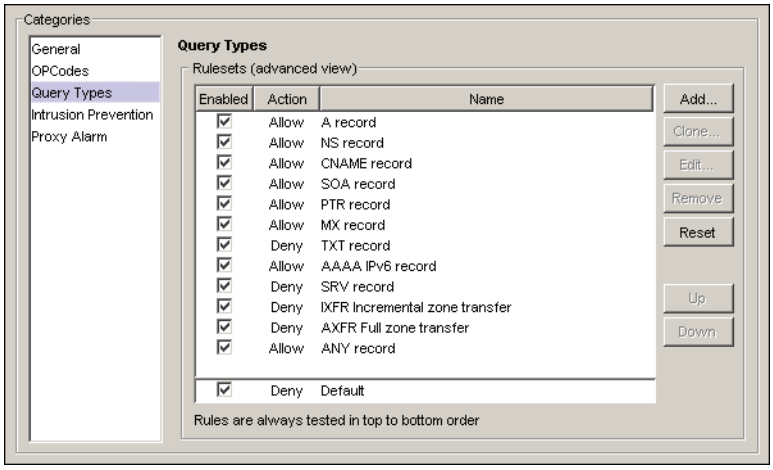
3 DNS OPcodes have an integer value. Use the arrows to set the OPCode value.
For more information on the integer values of DNS OPcodes, see RFC 1035.

4 Set an action for the rule and configure to send an alarm or enter the event in the log file. For more information, see "Adding rules" on page 80.

Configuring DNS query types

A DNS query type can configure a resource record by type (such as a CNAME or TXT record) or a custom type of query operation (such as an AXFR Full zone transfer). You can allow, deny, drop, or block specified DNS query types.

1 From the **Categories** section, select **Query Types.**



2 To enable a rule, select the **Enabled** check box adjacent to the action and name of the rule.

Adding a new query types rule

1 To add a new query types rule, click **Add**.
The New Query Types Rule dialog box appears.

2 Type a name for the rule.
Rules can have no more than 31 characters.

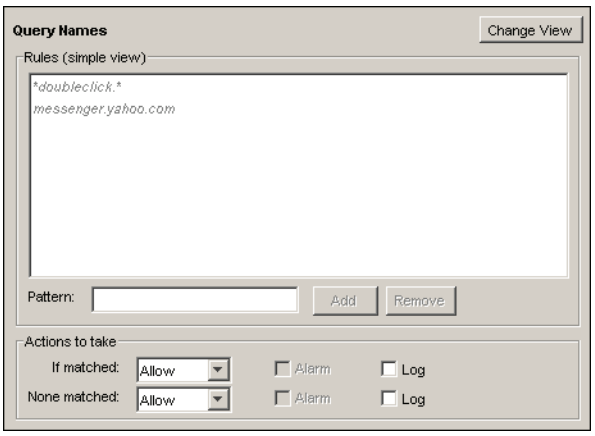
3 DNS query types have a resource record (RR) value. Use the arrows to set the value.
For more information on the values of DNS query types, see RFC 1035.

4 Set an action for the rule and configure to send an alarm or enter the event in the log file. For more information, see "Defining Rules" on page 79.

Configuring DNS query names

A DNS query name refers to a specified DNS domain name, shown as a fully qualified domain name (FQDN).

1 From the **Categories** section, select **Query Names.**



2 To add more names, do the steps used to create rules. For more information, see "Defining Rules" on page 79.

Enabling intrusion prevention for DNS

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

Configuring DNS proxy alarms

Use these settings to set criteria for a notification event:

1 From the **Categories** section, select **Proxy Alarm.**

2 Do the procedure in "Using dialog boxes for alarms, log messages, and notification" on page 83.

Configuring the TCP Proxy

Transmission Control Protocol (TCP) is the primary protocol in TCP/IP networks. The IP protocol controls packets while TCP enables hosts to start connections and to send and receive data. A TCP proxy monitors TCP handshaking to see if a TCP session is legitimate.

Configuring general settings for the TCP proxy

HTTP proxy action

Select the HTTP proxy action to use for TCP connections. The TCP proxy applies the HTTP proxy ruleset to all traffic that it identifies as HTTP traffic.

Send a log message with summary information for each transaction
Select this check box to record a log message for all TCP connection requests. This feature creates a large number of log messages and more traffic.

Enabling intrusion prevention for TCP

Although you can use the proxy definition screens to activate and configure IPS, it is easier to use **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the IPS screens in the proxy definition, see the chapter "Using Signature-Based Security Services."

CHAPTER 8

Working with Firewall NAT

Network Address Translation (NAT) was first developed as a solution for organizations that could not get enough registered IP network numbers from Internet Address Registrars for their increasing population of hosts and networks.

NAT is generically used to describe any of several forms of IP address and port translation. At its most basic level, NAT changes the IP address of a packet from one value to a different value. The primary purposes of NAT are to increase the number of computers that can operate off a single publicly routable IP address, and to hide the private IP addresses of hosts on your LAN.

There are different ways to use NAT. WatchGuard System Manager supports three different forms of NAT.

Dynamic NAT

Dynamic NAT is also known as IP masquerading. The Firebox can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network. Dynamic NAT is generally used to hide the IP addresses of internal hosts when they get access to public services.

1-to-1 NAT

1-to-1 NAT binds hosts behind your optional or trusted networks to external IP addresses. This type of NAT is used to give external computers access to your public, internal servers.

Static NAT for a policy

Also known as port forwarding, you configure static NAT when you configure policies, as described in "Configuring Policies," on page 63. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall.

It is possible that, in your configuration, you use more than one type of NAT. You can apply NAT as a global setting, or as a setting in a policy. Note that global NAT settings do not apply to BOVPN or MUVPN policies.

Using Dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the Firebox®. Outside the Firebox, you only see the IP address of the Firebox on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network.

In most networks, the recommended security policy is to apply NAT to all outgoing packets. With Fireware™, dynamic NAT is enabled by default in the **Network > Firewall NAT** dialog box. It is also enabled by default in each policy you create. You can override the global setting for Dynamic NAT in your individual policies.

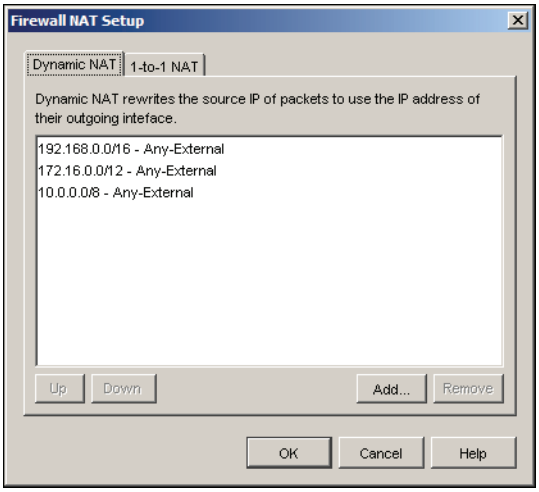
Adding global dynamic NAT entries

The default configuration of dynamic NAT enables dynamic NAT from all private IP addresses to the external network. The default entries are:

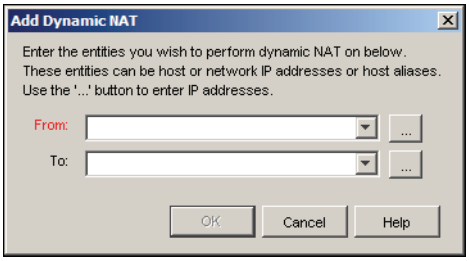
- 192.168.0.0/16 - Any-External
- 172.16.0.0/12 - Any-External
- 10.0.0.0/8 - Any-External

These three network addresses are the private networks reserved by the Internet Engineering Task Force (IETF). To enable dynamic NAT for private IP addresses other than these, you must add an entry for them. The Firebox® applies the dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list. We recommend that you put the rules in a sequence that matches the volume of traffic the rules apply to.

1 From Policy Manager, select **Network > Firewall NAT**.
The Firewall NAT Setup dialog box appears.



2 On the **Dynamic NAT** tab of the **Firewall NAT Setup** dialog box, click **Add**.
The Add Dynamic NAT dialog box appears.


Add Dynamic NAT
Enter the entities you wish to perform dynamic NAT on below.
These entities can be host or network IP addresses or host aliases.
Use the '...' button to enter IP addresses.
From:
To:
OK
Cancel
Help

3 Use the **From** drop-down list to select the source of the outgoing packets.
For example, use the trusted host alias to enable NAT from all of the trusted network. For more information on built-in Firebox aliases, refer to "Configuring the Firebox as an Authentication Server" on page 113.

4 Use the **To** drop-down list to select the destination of the outgoing packets.

5 To add a host or a network IP address, click the Add Device button shown at the right. Use the drop-down list to select the address type. Type the IP address or the range. You must type a network address in slash notation.
When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

6 Click **OK**.
The new entry appears in the Dynamic NAT Entries list.

Reordering dynamic NAT entries

To change the sequence of the dynamic NAT entries, select the entry to change. Then click **Up** or **Down**.

You cannot change a dynamic NAT entry. If a change is necessary, you must erase the entry with **Remove**. Use **Add** to enter it again.

Policy-based dynamic NAT entries

With this type of NAT, the Firebox uses the primary IP address of the outgoing interface for the outgoing packets for this policy. Each policy has dynamic NAT enabled by default, which uses the global dynamic NAT table. To disable dynamic NAT for all traffic in a policy:

Disabling policy-based dynamic NAT

1 From Policy Manager, right-click a policy and select **Edit**.
The Edit Policy Properties window appears.

2 Click the **Advanced** tab.

3 Clear the check box in front of Dynamic NAT to turn NAT off for the traffic this policy controls.

4 Click **OK**. Save the change to the Firebox.

Using 1-to-1 NAT

When you enable 1-to-1 NAT, the Firebox changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses. You can configure up to 64 different 1-to-1 NAT addresses. This allows you to configure a 1-to-1 NAT rule for a single /26 network, or a total of 64 IP addresses among all 1-to-1 NAT rule entries. A 1-to-1 NAT rule always takes precedence over dynamic NAT.

1-to-1 NAT is frequently used when you have a group of internal servers with private IP addresses that must be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers. You do not have to change the IP address of your internal servers. When you have a group of similar servers (for example, a group of e-mail servers), 1-to-1 NAT is easier to configure than static NAT for the same group of servers.

To understand how to configure 1-to-1 NAT, we give this example:

Company ABC has a group of five privately addressed e-mail servers behind the trusted interface of their Firebox X Peak. These addresses are:

10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
10.1.1.5

Company ABC selects five public IP addresses from the same network address as the external interface of their Firebox, and creates DNS records for the e-mail servers to resolve to. These addresses are:

50.1.1.1
50.1.1.2
50.1.1.3
50.1.1.4
50.1.1.5

Company ABC configures a 1-to-1 NAT rule for their e-mail servers. The 1-to-1 NAT rule builds a static, bi-directional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.1.1.1 <--> 50.1.1.1
10.1.1.2 <--> 50.1.1.2
10.1.1.3 <--> 50.1.1.3
10.1.1.4 <--> 50.1.1.4
10.1.1.5 <--> 50.1.1.5

When the 1-to-1 NAT rule is applied, the Firebox creates the bi-directional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.

Defining a 1-to-1 NAT rule

In each 1-to-1 NAT policy you can configure a host, a range of hosts, or a subnet. You must also configure:

Interface

The name of the Firebox® Ethernet interface on which 1-to-1 NAT is applied. The Firebox will apply 1-to-1 NAT for packets sent in to, and out of, the interface. In our example above, the rule is applied to the external interface.

NAT base

When you configure a 1-to1 NAT policy, you configure the policy with a “from” and a “to” range of IP addresses. The NAT base is the first available IP address in the “to” range of addresses. The NAT base IP address is the address that the real base IP address changes to when the 1-to-1 NAT is applied. In our example above, the NAT base is 50.1.1.1.

Real base

When you configure a 1-to1 NAT policy, you configure the policy with a "from" and a "to" range of IP addresses. The Real base is the first available IP address in the "from" range of addresses. It is the IP address assigned to the physical Ethernet interface of the computer to which you will apply the 1-to-1 NAT policy. When packets from a computer with a real base address go through the interface specified, the 1-to-1 action is applied. In our example above, the Real base is 10.1.1.1.

Number of hosts to NAT (for ranges only)

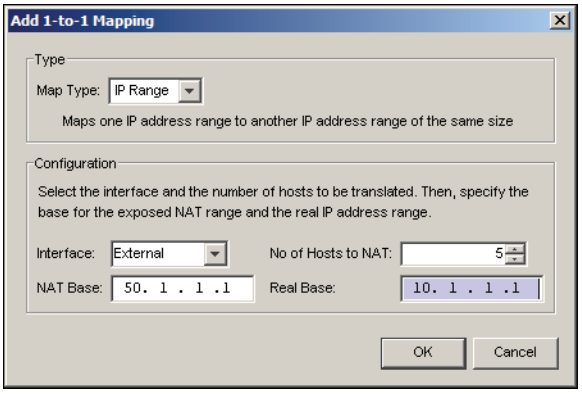
The number of IP addresses in a range to which the 1-to-1 NAT rule applies. The first real base IP address is translated to the first NAT Base IP address when 1-to-1 NAT is applied. The second real base IP address in the range is translated to the second NAT base IP address when 1-to-1 NAT is applied. This is repeated until the "Number of hosts to NAT" is reached. In our example above, the number of hosts to NAT is five.

You can also use 1-to-1 NAT to solve the problem when you must create a VPN tunnel between two networks that use the same private network address. When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT. Then, you can create the VPN tunnel and not change the IP addresses of one side of the tunnel.

Configuring global 1-to-1 NAT

1 From Policy Manager, click **Setup > Firewall NAT**. Click the **1-to-1 NAT** tab.

2 Click **Add**.
The 1-1 Mapping dialog box appears.


Add 1-to-1 Mapping
Type
Map Type:
IP Range
Maps one IP address range to another IP address range of the same size
Configuration
Select the interface and the number of hosts to be translated. Then, specify the base for the exposed NAT range and the real IP address range.
Interface:
External
No of Hosts to NAT:
5
NAT Base:
50. 1 . 1 .1
Real Base:
10. 1 . 1 .1
OK
Cancel

3 In the **Map Type** drop-down list, select **Single IP**, **IP range**, or **IP subnet** to configure if you want to map to one host, a range of hosts, or a subnet.

4 In the **NAT base** text box, type the address for the NAT range to see externally.

5 Complete all the information. Click **OK**.

6 Repeat steps 2 - 4 for each 1-to-1 NAT entry. When you are done, click **OK** to close the **Firewall NAT Setup** dialog box. Save the change to the Firebox.

After you configure global 1-to-1 NAT rule, you must configure the NAT base IP addresses in the appropriate policies. In the example given above, we must configure our SMTP policy to allow SMTP traffic from Any to 50.1.1.1-50.1.1.5.

Configuring policy-based 1-to-1 NAT

With this type of NAT, the Firebox uses the private and public IP ranges that you set when you configured global 1-to-1 NAT, but the rules are applied to an individual policy. 1-to-1 NAT is enabled in the default configuration of each policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, the 1-to-1 NAT gets precedence. 1-to-1 NAT will not disable dynamic NAT for the policy.

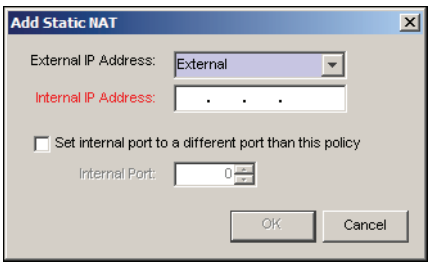
Disabling policy-based 1-to-1 NAT

1 From Policy Manager, right-click a policy and select **Edit**.
2 The **Edit Policy Properties** window appears.
3 Click the **Advanced** tab.
4 Clear the **1-to-1 NAT** check box to turn NAT off for the traffic this policy controls.
5 Click **OK**. Save the change to the Firebox.

Configuring Static NAT for a Policy

Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall. Because of how static NAT works, it is available only for policies that use a specified TCP or UDP port. A policy that has another protocol cannot use incoming static NAT. If you have a policy that uses a protocol other than TCP or UDP, the **NAT** button in the **Properties** dialog box of that policy is disabled. You also cannot use Static NAT with the Any policy.

1 Double-click a policy icon in the Policies Arena.
2 From the **Connections are** drop-down list, select **Allowed**.
To use static NAT, the policy must let incoming traffic through.
3 Below the **To** list, click **Add**.
The Add Address dialog box appears.
4 Click **NAT**.
The Add Static NAT dialog box appears.



5 From the **External IP Address** drop-down list, select the "public" address to use for this service.
6 Type the internal IP address.
The internal IP address is the destination on the trusted or optional network.
7 If necessary, select the **Set internal port to different port than this policy** check box.
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host but also to a different port. If you select the check box, type the different port number or use the arrow buttons in the Internal Port box.
8 Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.

9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Properties** dialog box of the service.

CHAPTER 9

Implementing Authentication

With user authentication you can see user names when you monitor the connections through the Firebox®. Without authentication, you see only the IP address of each connection. With authentication, you see the user name and IP address of each Firebox connection. As a result, a person can log in to the network from any computer, but see only the information for which they have authentication. All the connections that the user starts from that IP address also transmit the session name while the user is authenticated.

The Firebox allows you to create policies that include groups and user names. As a result, the policy is applied to any computer a person uses to log in. Monitor by user name:

- If you use the Dynamic Host Configuration Protocol (DHCP), because the IP address of a computer can change.
- If many different users can use the same IP address in a day.

In these cases, authentication gives you more information about the employee actions.

How User Authentication Works

A special HTTPS server operates on the Firebox® to accept authentication requests. To authenticate, a person must connect to the authentication Web page on the Firebox. The address is:

https://*IP address of a Firebox interface*:4100/

An authentication Web page appears. A person must type their user name and password. The Firebox sends the name and password to the authentication server using PAP (Password Authentication Protocol). When the user is authenticated, the user is then allowed to use the approved network resources. A person is authenticated for two hours after they close their last authenticated connection.

To close an authenticated session before two hours, click **Logout** on the Authentication Web page. If the page is closed, you must open it again to disconnect. To prevent an account from authenticating, you must disable the account on the authentication server.

Using authentication from the external network

The primary function of the authentication tool is to authenticate outgoing traffic. You can also use it for incoming network traffic. When you have an account on the Firebox, you can always use external

authentication. For example, you can type this address in your browser at home: https://public IP address of a Firebox interface:4100/

After you authenticate, you can use the policies that are configured on the Firebox (FTP, Telnet).

Use this procedure to let a remote user authenticate from the external interface. This lets the person use resources through the Firebox.

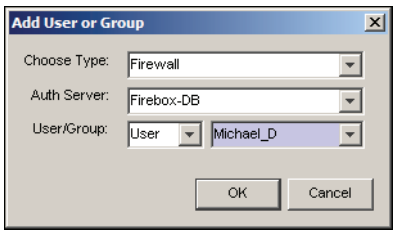
1 From Policy Manager, double-click the **WatchGuard Authentication** policy icon. This policy appears after you add a user or group to a policy configuration.

2 Click the **Policy** tab.

3 From the **WG-Auth connections are** drop-down list, select **Allowed**.

4 Below the **From** box, click **Add**.

5 Click **Add User.** From the **User/Group** drop-down list, select **User** or **Group**, and then select the name you want from the adjacent drop-down list.



Using authentication through a gateway Firebox to another Firebox

To send an authentication request through a gateway Firebox to a different Firebox, you must add a policy that allows the authentication traffic on the gateway Firebox. On the gateway Firebox, use Policy Manager to add the WatchGuard Authentication policy. This policy controls traffic on TCP port 4100. Configure the policy to allow traffic to the IP address of the destination Firebox.

Authentication server types

With Fireware, there are five authentication methods:

- Firebox
- RADIUS
- SecurID
- LDAP
- Active Directory

You can configure one or more authentication server types for a Firebox. Authentication to different server types is almost the same for the user. For the Firebox administrator, the difference is that the user database can be on the Firebox or on a dedicated authentication server.

When you use an authentication server, you configure it with the instructions from its manufacturer. You install the server with access to the Firebox and put it behind the Firebox for security.

Using a backup authentication server

You can configure a backup authentication server with all types of third-party authentication. If the Firebox cannot connect to the primary authentication server (after three attempts), it connects to the backup authentication server. If the Firebox cannot connect to the backup authentication server, it waits

ten minutes, and then tries to connect to the primary authentication server again. This cycle continues until the Firebox connects with an authentication server.

Configuring the Firebox as an Authentication Server

If you do not use a third-party authentication server, you can use the Firebox® as an authentication server. This procedure divides your company into groups and users for authentication. The group to which you assign a person is controlled by the tasks they do and information they use. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new persons group, with controlled access to the Internet.

In a group, you set the authentication procedure for the users, the system type, and the information to which they have access. A user can be a network or a computer. If your company changes, you can add or remove users or systems from your groups.

Use Policy Manager to:

- Add, change, or erase the groups in the configuration
- Add or change the users in a group

About Firebox authentication

You can configure the Firebox to authenticate users for three different types of authentication:

- Firewall authentication
- PPTP connections
- MUVPN connections

When the authentication is successful, the Firebox makes a mapping between these items:

- User name
- The Firebox User group (or groups) of which the user is a member
- The IP address on the user's computer when the user authenticates

Firewall authentication

You use Firewall authentication to disallow access to network resources. You make a Firebox user account at **Setup > Authentication Servers**. After you make the user account, you can make a Firebox group and you can put the user in that Firebox User group.

Next, you make a policy that only allows traffic from or to [a list of Firebox User names] or [a list of Firebox groups]. The Firebox does not look at this policy unless it comes from or goes to the authenticated user's IP address.

A user authenticates by making an HTTPS connection to the Firebox over port 4100. The user puts this address into the browser and completes the authentication screen:
https://[firebox.ip.address]:4100
If the user name and password match an entry in the Firebox User database, the user is authenticated.

Traffic that comes from or goes to this user's computer matches a policy if the user name, a group of which the user is a member, or the IP address on the computer from which the user authenticated is in the policy.

PPTP connections

You configure the Firebox to host PPTP VPN sessions. To do this, select **VPN > Remote Users** and click the **PPTP** tab. If you do not select the check box **Use RADIUS Authentication to authenticate remote users**, then the Firebox authenticates the PPTP session. The Firebox checks to see if the user name and password the user puts into the VPN connection box matches the user name and password in the Firebox User database. If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.

Next, you make a policy that only allows traffic From or To [a list of Firebox User names] or [a list of Firebox Groups]. The Firebox does not look at this policy unless traffic comes from or goes to the authenticated user's virtual IP address.

The user makes the PPTP connection using the built-in PPTP capability of the computer. If the user name and password match an entry in the Firebox User database, the user is authenticated and the Firebox allows the PPTP connection. However, traffic from the authenticated user is allowed only if there is a policy for it.

Because the Firebox allows the PPTP connection from any Firebox user that gives the proper credentials, it is important that you make a policy for PPTP sessions that lists only users you allow to pass traffic over the PPTP session. Or, put these users into a special Firebox User group and make a policy that allows traffic only from this group. The Firebox has a pre-configured group for this called "PPTP-Users". It is recommended that you use this group only in a policy that allows traffic from users you allow to pass traffic over a PPTP session.

MUVPN connections

You can configure the Firebox to host MUVPN IPSec VPN sessions. To do this, select **VPN > Remote Users** and click the **Mobile User VPN** tab. You make the MUVPN group using a wizard. When the wizard is fin-ished, the Policy Manager does two things:

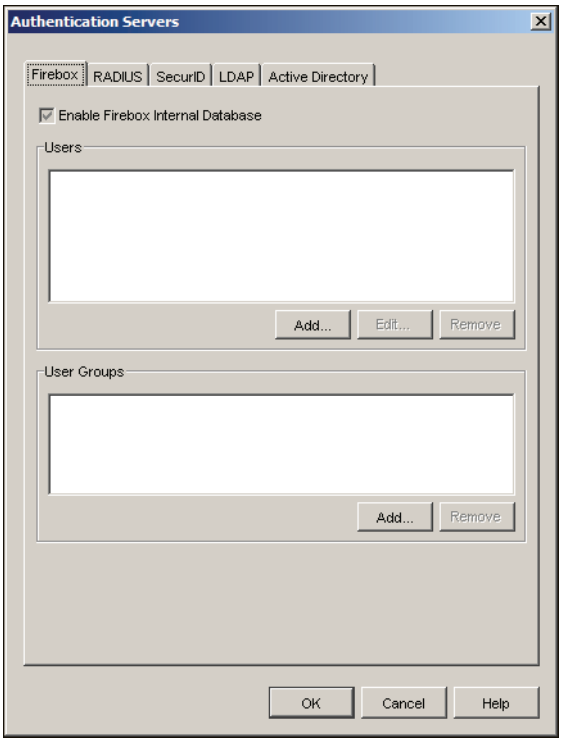
It makes a client configuration profile (called a .wgx file) and puts it on the management station computer that created the MUVPN account. The user must have this .wgx file to configure the MUVPN client computer.

It automatically adds an "Any" policy to the **Mobile User VPN** tab that allows traffic to pass from the authenticated MUVPN user.

When the user's computer is properly configured, the user makes the MUVPN connection. If the user name and password the user puts into the MUVPN authentication applet match an entry in the Firebox User database, and if the user is in the MUVPN group you create, the MUVPN session is authenticated. Policy Manager automatically makes a policy that allows any traffic from the authenticated user. You can delete the "Any" policy if you do not want to allow the MUVPN client to pass traffic over any port. To restrict the ports the MUVPN client can access, add policies for those ports to the **Mobile User VPN** tab. To learn how to add policies, see the "Configuring Policies" chapter.

Setting up the Firebox as an authentication server

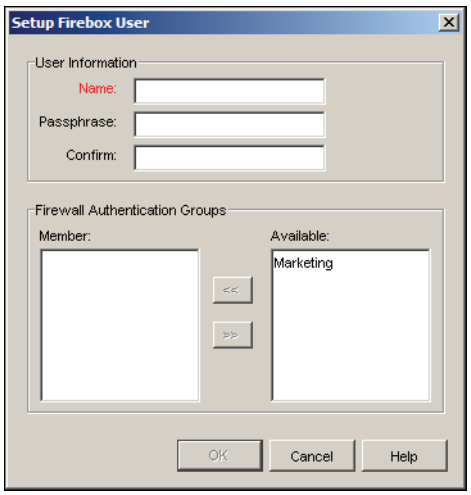
1 From Policy Manager, select **Setup > Authentication Servers**.
The Authentication Servers dialog box appears. The default configuration enables the Firebox authentication server.



2 To add a new user group, click **Add** below the **User Groups** list.
The Add Firebox Group dialog box appears.

3 Type the group name that you want. Click **OK**.

4 To add a new user, click **Add** below the **Users** list.
The Setup Firebox User dialog box appears.



5 Type the name and the passphrase you want the person to use to authenticate to the Firebox.
When this passphrase is set, you cannot see the passphrase in simple text again. If you lose the passphrase, you must set a new passphrase.

6 To add the user to a group, select the group name in the **Available** list. Click the double arrow that points left to move the name to the **Member** list.
You can also double-click the Group name.

7 Add the user to the PPTP-Users group if you want to use the PPTP-Users group in a service.

8 After you add the user to selected groups, click **OK**.
The user adds to the User list. You can then add more users.

9 To close the **Setup Firebox User** dialog box, click **OK**.
The Firebox Users tab appears with a list of the new users.

10 After you add all necessary users and groups, click **OK**.
At this time, you can use the users and groups to configure policies and authentication.

Using a local user account for Firewall user, PPTP and MUVPN authentication

Local user accounts can perform Firewall user, PPTP, and MUVPN authentication, even the accounts are not associated with a specific authentication group. For example, a local user account that is configured to belong to the FW-Users group onlycan authenticate and bring up a PPTP or MUVPN tunnel if PPTP or MUVPN is enabled on the appliance.

However, after an authentication or tunnel has been successfully established, only legitimately authenticated users for a specific authentication group can send traffic through the corresponding matching policy. For example, an MUVPN-only user can send traffic through an MUVPN tunnel, but not a PPTP tunnel even though the user can authenticate and bring up a PPTP tunnel.

1 Enable and configure firewall user authentication, MUVPN, and PPTP to use local accounts.

2 Create appropriate policies for these authentication types.

3 Associate an user account to each authentication group (FW-Users, PPTP-Users, MUVPN-Users). Also create an account that does not belong to any group.

4 Deploy the configuration to the appliance.

5 Use a web browser, PPTP client, and MUVPN client to authenticate to the Firebox using each of these user accounts.

Configuring RADIUS Server Authentication

Remote Authentication Dial-In User Service (RADIUS) authenticates the local users and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, and VPN gateways in one database.

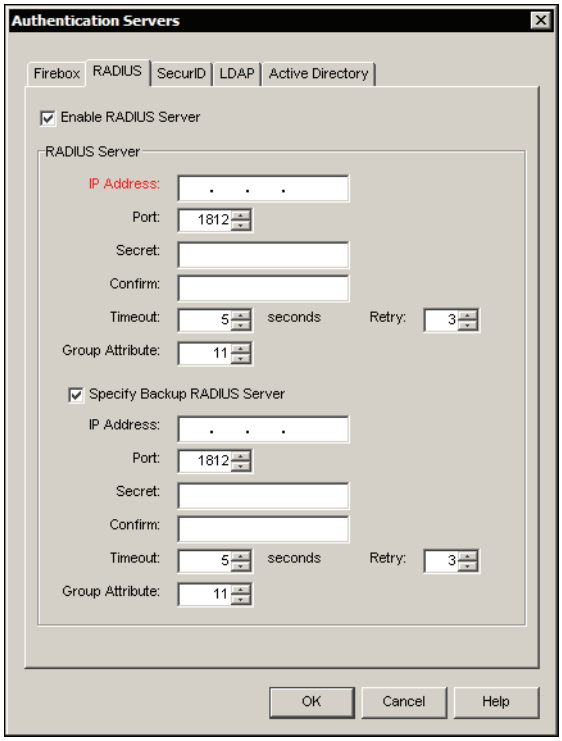
The authentication messages to and from the RADIUS server always use an authentication key. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, hackers cannot get to the authentication messages. Note that RADIUS sends a key, and not a password, during authentication. For Web and MUVPN authentication, RADIUS gives support only to PAP (not CHAP) authentication. For authentication with PPTP, RADIUS gives support only to MSCHAPv2.

To use RADIUS server authentication with the Firebox®, you must:

- Add the IP address of the Firebox to the RADIUS server, as described in the RADIUS documentation.
- Enable and specify the RADIUS server in your Firebox configuration.
- Add RADIUS user names or group names into the policies in Policy Manager.

To enable RADIUS Server Authentication:

1 From Policy Manager, select **Setup > Authentication Servers**. Click the **RADIUS Server** tab.
The RADIUS configuration appears.



2 In the **IP Address** box, type the IP address of the RADIUS server.

3 In the **Port** box, make sure that the port number RADIUS uses for authentication appears.
The default port number is 1812. Older RADIUS servers may use port 1645.

4 In the **Secret** box, type the "shared secret" between the Firebox and the RADIUS server.
The shared secret is a password that is case-sensitive, and it must be the same on the Firebox and the RADIUS server.

5 To set the time-out value, use the **Timeout** value control to set the value you want.
This sets how long the Firebox waits for a response from the authentication server before it tries to connect again.

6 To set how many connection attempts the Firebox makes, use the **Retry** value control to set the number you want.

This is the number of times the Firebox tries to connect to the authentication server (using the time-out specified above) before it reports a failed connection for one authentication attempt.

7 To set the group attribute, use the **Group Attribute** value control to set the attribute you want.

The group attribute value is used to set which attribute carries the User Group information. When the RADIUS server sends a message to the Firebox that a user is authenticated, it also sends a User Group string, for example "engineerGroup" or "financeGroup". This information is then used for access control.

8 To add a backup RADIUS server, select the **Specify Backup RADIUS Server** check box. If you select the check box, type the IP address and the port of the backup RADIUS server. The shared secret must be on the primary and backup RADIUS server.

9 Click **OK**.

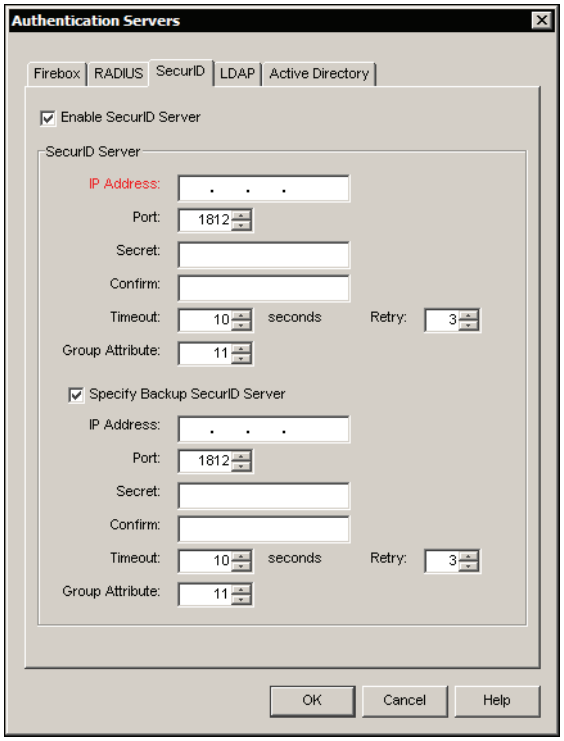
Configuring SecurID Authentication

To operate SecurID authentication, you must configure RADIUS and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN (personal identification number). Refer to the SecurID instructions for more information.

Note

Do not use Steel Belted RADIUS with SecurID. Use the RADIUS software application with RSA SecurID software.

1 From Policy Manager, select **Setup > Authentication Servers**. Click the **SecurID Server** tab.



2 In the **IP Address** box, type the IP address of the SecurID server.

3 In the **Port** box, use the value control to the port number for SecurID authentication you want.
The default number is 1812.

4 In the **Secret** box, type the "shared secret" between the Firebox® and SecurID server.
The shared secret is a case-sensitive password and must be the same on the Firebox and SecurID server.

5 In the **Timout** box, use the value control to select the timeout value you want.
This sets how long the Firebox waits for a response from the authentication server before it tries to connect again.

6 To set how many connection attempts the Firebox makes, use the **Retry** value control to set the number you want.
This is the number of times the Firebox tries to connect to the authentication server (using the time-out specified above) before it reports a failed connection for one authentication attempt.

7 Select the group attribute.
The group attribute value is used to set which attribute carries the User Group information. When the SecurID server sends a message to the Firebox that a user is authenticated, it also sends a User Group string, for example "engineerGroup" or "financeGroup". This information is then used for access control.

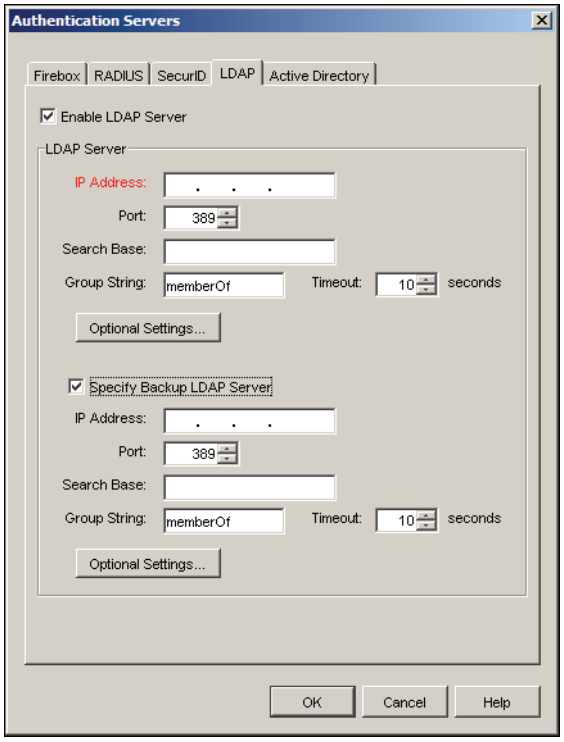
8 Type the IP address and the port of the backup SecurID server. The shared secret must be on the primary and backup SecurID server.

9 Click **OK**.

Configuring LDAP Authentication

You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users to the Firebox®. LDAP is an open-standard protocol for using online directory services, and it operates with Internet transport protocols, such as TCP. You can use LDAP to get access to stand-alone directory servers or X.500 directories. You must configure the Firebox and configure the LDAP server.

1 From Policy Manager, select **Setup > Authentication Servers**. Select the **LDAP** tab.



2 Select the **Enable LDAP Server** check box.

3 In the **IP Address** box, type the IP address of the primary LDAP server for the Firebox to contact with authentication requests.

4 From the **Port** drop-down list, select the TCP port number for the Firebox to use to connect to the LDAP server. The default port number is 389.

5 Type the **Search Base**.
Supply an LDAP search base to identify the organizational unit to search for authentication matches.

6 Type the **Group String**.
The attribute string that is used to hold user group information on the LDAP server. On many LDAP servers, the default group string is "uniqueMember".

7 If necessary, change the time-out value. This is how long the Firebox waits for a response from the authentication server.

8 Add information for a backup LDAP Server, if you have one.

9 To configure MUVPN users to get authentication information from the LDAP Server, click the **Optional Settings** button. You can enter MUVPN client information in the user properties of your LDAP Server, which includes the IP address, subnet mask, or DNS and WINS servers. Then, you can map these fields to the fields that appear in Optional Settings. When the MUVPN user start a VPN tunnel through the Firebox, the Firebox sets the IP address, subnet mask, or DNS and WINS servers for the user with the information contained in the LDAP user properties.

IP *Attribute String*
Type the name of the LDAP user property field name that contains the assigned IP address.

Netmask Attribute String
Type the name of the LDAP user property field name that contains the assigned subnet mask.

DNS Attribute String
Type the name of the LDAP user property field name that contains the DNS server IP address.

WINS Attribute String
Type the name of the LDAP user property field name that contains the WINS server IP address.

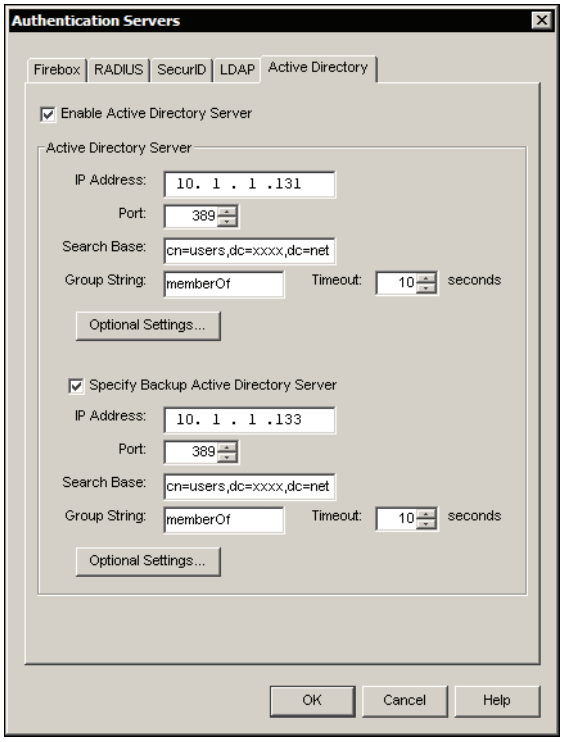
Lease Time Attribute String
Type the name of the LDAP user property field name that contains the total time allowed for the MUVPN connection session.

Idle Timeout Attribute String
Type the name of the LDAP user property field name that contains the assigned idle timeout.

Configuring Active Directory Authentication

You can use an Active Directory authentication server to authenticate your users to the Firebox. You must configure the Firebox® and configure the Active Directory server.

1 From Policy Manager, select **Setup > Authentication Servers**. Select the **Active Directory** tab



2 Select the **Enable Active Directory Server** check box.

3 Type the IP address of the primary Active Directory server to which the Firebox sends authentication requests.

4 Select the TCP port number for the Firebox to use to connect to the Active Directory server. The default port number is 389.

5 Type the **Search Base**. The standard format for the search base setting is: cn=common name,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after a "dot".
For example, if your user accounts are in an OU (organizational unit) you refer to as "accounts" and your domain name is HQ_main.com. Your search base is: "ou=accounts,dc=HQ_main,dc=com".
You set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.

6 Type the **Group String**.
The attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always "memberOf".

7 If necessary, change the time-out value. This is the time the Firebox waits for a response from the authentication server.

8 Add information for a backup Active Directory Server, if you have one.

9 To configure MUVPN users to get authentication information from the Active Directory Server, click the **Optional Settings** button. You can enter MUVPN client information in the user properties of your Active Directory Server, which includes as the IP address, subnet mask, or DNS and WINS

servers. Then, you can map these fields to the fields that appear in Optional Settings. When the MUVPN user starts a VPN tunnel through the Firebox, the Firebox sets the IP address, subnet mask, or DNS and WINs servers for the user with the information that appears in the Active Directory user properties.

IP Attribute String
: Type the name of the Active Directory user property field name that contains the assigned IP address.

Netmask Attribute String
: Type the name of the Active Directory user property field name that contains the assigned subnet mask.

DNS Attribute String
: Type the name of the Active Directory user property field name that contains the DNS server IP address.

WINS Attribute String
: Type the name of the Active Directory user property field name that contains the WINS server IP address.

Lease Time Attribute String
: Type the name of the Active Directory user property field name that contains the assigned lease time.

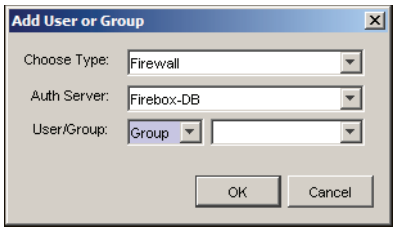
Idle Timeout Attribute String
: Type the name of the Active Directory user property field name that contains the assigned idle timeout.

Configuring a Policy with User Authentication

When you configure the Firebox® to use an authentication server, you can start to use user names when creating policies in Policy Manager. One method you can use is to put a limit on all policies that connections are allowed only for authenticated users. This helps when you use DHCP on your network.

1 Create a group on your third-party authentication server that contains all the user accounts.

2 In Policy Manager, add or start your Outgoing policy. Below the **From** field, click **Add** and then click **Add User**.
The Add User or Group dialog box appears.



3 From the **Choose Type** drop-down list, select firewall, MUVPN, or PPTP authentication.

4 From the **Auth Server** drop-down list, select the type of authentication server to use.

5 From the **User/Group** drop-down list, select **User** or **Group**.

6 Type the user or group name you created on the authentication server. Click **OK**.

7 Configure the **From** fields on all policies in Policy Manager the same way.

8 After you add a user or group to a policy configuration, use the WatchGuard Authentication policy that appears in Policy Manager to control access to the authentication Web page.

CHAPTER 10

Firewall Intrusion Detection and Prevention

WatchGuard® Fireware™ and the policies you create in Policy Manager give you strict control over access to your network. A strict access policy helps keep hackers out of your network. But, there are other types of attacks that a strict policy cannot defeat. Careful configuration of the Firebox® default packet handling options can stop attacks such as SYN flood attacks, spoofing attacks, and port or address space probes.

With default packet handling, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If there is a risk, you can configure the Firebox to automatically block against the possible attack. This proactive method of intrusion detection keeps attackers out of your network. You can also purchase an upgrade for your Firebox to use signature-based intrusion prevention. For more information, see the chapter "Signature-Based Intrusion Detection and Prevention" in this Configuration Guide.

Using Default Packet Handling Options

The firewall examines the source and destination of each packet it receives. It looks at the IP address and the port number. The firewall also monitors the packets to look for patterns that can show that your network is at risk.

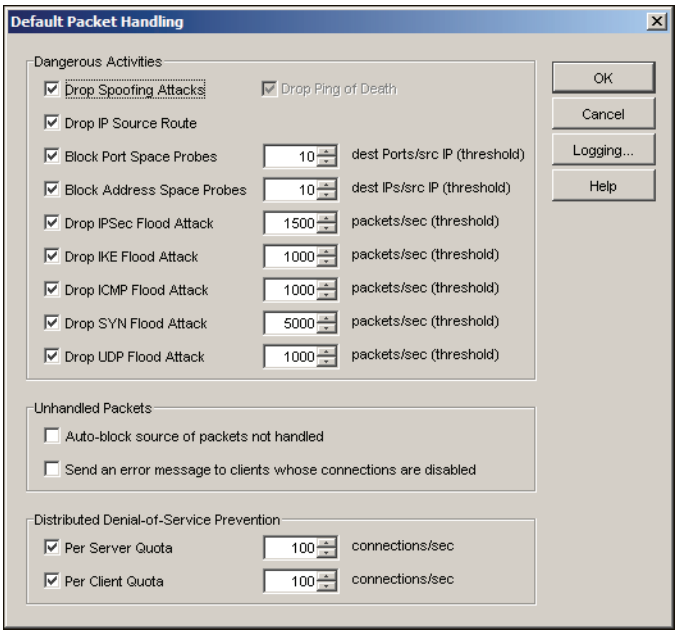
Default packet handling:

- Rejects a packet that can be a security risk
- Can automatically block all traffic to and from a source IP address
- Adds an event to the log file
- Sends an SNMP trap to the SNMP management server
- Sends a notification of possible security risks

You set all default packet handling options with the **Default Packet Handling** dialog box.

1 From Policy Manager, select **Setup > Intrusion Prevention > Default Packet Handling**.
or,
Click the default packet handling icon on the Policy Manager toolbar.
The Default Packet Handling dialog box appears.

2 Select the check box for the traffic patterns you want to prevent, as explained in the sections that follow. The default configuration sends a log message when one of these events occur. To configure an SNMP trap or notification for default packet handling, click **Logging**.



Spoofing attacks

One procedure that attackers use to get access to your network is to make an "electronic false identity." With this "IP spoofing" procedure, the attacker sends a TCP/IP packet that uses a different IP address than the host that first sent it.

With IP spoofing enabled, the Firebox® checks to make sure that the source IP address of a packet is from a network on that interface.

To protect against spoofing attacks, select the **Drop Spoofing Attacks** check box from the **Default Packet Handling** dialog box.

IP source route attacks

Attackers use IP source route attacks to send an IP packet to find the route that the packet uses to go through the network. The attacker can then see the response to the packets and get information about the operating system of the target computer or network.

To protect against IP source route attacks, select the **Drop IP Source Route** check box from the **Default Packet Handling** dialog box.

"Ping of death" attacks

"Ping of death" is a denial of service (DoS) attack. It is caused by an attacker that sends an IP packet that is larger than the 65,535 bytes allowed by the IP protocol. This causes some operating systems to crash or restart.

To protect against ping of death attacks, the **Drop Ping of Death** feature is always enabled. You cannot disable this feature.

Port space and address space attacks

Attackers use probes to find information about networks and their hosts. Port space probes examine a host to find the services that it uses. Address space probes examine a network to see which hosts are on that network.

To protect against port space and address space attacks, select the **Block Port Space Probes** and the **Block Address Space Probes** check boxes from the **Default Packet Handling** dialog box. You then use the arrows to select the maximum allowed number of IP addresses or port probes for each source IP address.

Flood attacks

In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives sufficient ICMP ping commands that it uses all of its resources to send reply commands. The Firebox can protect against these types of flood attacks:

- IPSec flood attacks
- IKE flood attacks
- ICMP flood attacks
- SYN flood attacks
- UDP flood attacks

Flood attacks are also known as Denial of Service (DoS) attacks. You can use the **Default Packet Handling** dialog box to configure the Firebox to protect against these attacks. Select the check boxes for the flood attacks you want to prevent. Use the arrows to select the maximum allowed number of packets each second.

Unhandled Packets

An "unhandled" packet is a packet that does not match any rule created in Policy Manager. The Firebox always denies the packet, but you can also select to always automatically block the source. This adds the IP address that sent the packet to the temporary blocked sites list. You can also send a TCP reset or ICMP error back to the client when an unhandled packet is received by the Firebox.

Distributed denial of service attacks

Distributed Denial of Service (DDoS) attacks are almost the same as flood attacks. In a DDoS, the ICMP ping commands come from many computers. You can use the **Default Packet Handling** dialog box to configure the Firebox to protect against DDoS attacks. Use the arrow keys to set the maximum allowed number of connections that your servers and clients can receive each second.

Setting Blocked Sites

The Blocked Sites feature helps prevent network traffic from systems you know or think are dangerous or a security risk. After you find the source of suspicious traffic, you can block all the connections with that IP address. You can also configure the Firebox to send a log message each time the source tries to connect to your network. From the log file, you can see the services that they use to attack.

A blocked site is an IP address that cannot make a connection through the Firebox. If a packet comes from a system that is blocked, it does not get through the Firebox®.

There are two different types of blocked IP addresses:

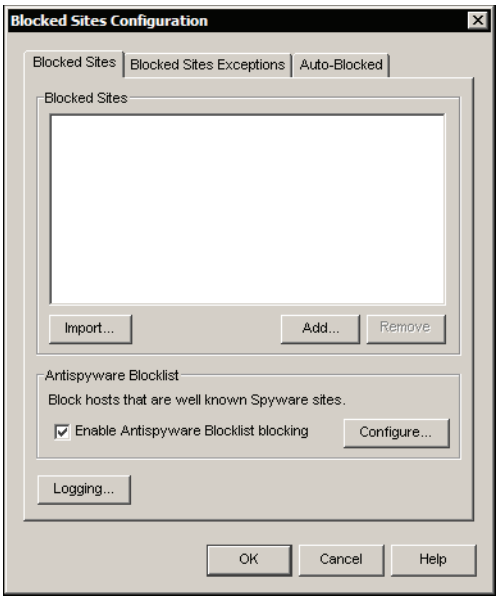
- Permanently blocked sites — on a list in the configuration file that you set manually.
- Auto-blocked sites — The IP addresses that the Firebox adds or removes on a temporary blocked site list. The Firebox uses the packet handling rules that are specified for each service. For example, you configure the Firebox to block the IP addresses that try to connect to a blocked port. These addresses are then blocked for a specified time.

You can use a list of temporarily blocked sites with log messages to help you make a decision about which IP addresses to block permanently.

Blocking a site permanently

You use Policy Manager to permanently block a host that you know is a security risk. For example, a university computer that hackers use frequently is a good host to block.

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Sites**.
The Blocked Sites Configuration dialog box appears.



2 Click **Add**.
The Add Site dialog box appears.

3 Use the **Choose Type** drop-down list to select a member type. The selections are **Host IP, Network IP** or **Host Range**.

4 Type the member value.
The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the tab or the arrow key.

5 Select **OK**.
The new site appears in the Blocked Sites list.

Using an external list of blocked sites

You can make a list of blocked sites in an external file. This file must be a `.txt` file. To add an external file to your blocked sites list:

1 In the **Blocked Sites Configuration** dialog box, select **Import**.

2 Find the file. Double-click it, or select it and select **Open**.
The sites in the file appear in the Blocked Sites list.

Creating exceptions to the Blocked Sites list

A host that is a blocked sites exception does not appear in the list of automatically blocked sites. The automatic rules do not apply for this host.

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Sites**.

2 Click the **Blocked Sites Exceptions** tab. Click **Add.**

3 Use the **Choose Type** drop-down list to select a member type. The selections are **Host IP, Network IP** or **Host Range**.

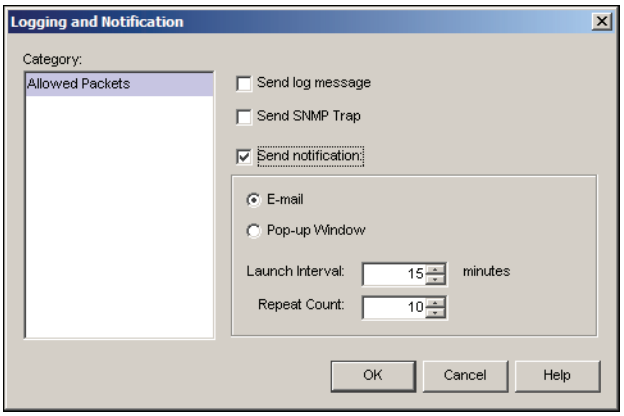
4 Type the member value.
The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the TAB or the arrow key.

5 Select **OK**.

Setting logging and notification parameters

You can configure the Firebox to make a log entry when a host tries to use a blocked site. You can also set up notification for when a host tries to get access to a blocked site.

1 From the **Blocked Sites** dialog box, select **Logging**.
The Logging and Notification dialog box appears.



2 Set the parameters and notification to comply with your security policy:

Enter it in the log

When you enable this check box, the Firebox sends a log message when a packet is denied because of your blocked port configuration. The default configuration of all services is for the Firebox to send a log message when it denies a packet.

Send SNMP trap

When you enable this check box, the Firebox sends an event notification to the SNMP management system. The SNMP trap makes sure that traffic matches allowed values. An example of a criteria it examines is a threshold limit.

Send notification

When you enable this check box, the Firebox sends a notification when a packet is denied because of your blocked port configuration. You can configure the Firebox to do one of these actions:

- **E-mail** The Firebox sends an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the Log Server user interface.
- **Pop-up Window** The Firebox makes a dialog box appear on the management station when the event occurs.

Setting Launch Interval and Repeat Count

You can control the time of the notification, together with the Repeat Count, as follows:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

Repeat Count

This counts how frequently an event occurs. When this gets to the selected value, a special repeat notifier starts. This notifier makes a repeat log entry about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are configured as:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 a.m. and continues each minute. This starts the logging and notification mechanisms. These are the times and the actions that occur:

1 10:00—Initial port space probe (first event)

2 10:01—First notification starts (one event)

3 10:06—Second notification starts (reports five events)

4 10:11—Third notification starts (reports five events)

5 10:16—Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notifier.

Blocking sites temporarily with policy settings

You can use the policy configuration to block sites that try to use a denied service:

1 From Policy Manager, double-click the policy icon.
The Properties dialog box appears.

2 On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied**.

3 On the **Properties** tab, select the check box **Automatically block sites that attempt to connect**.

Blocking Ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. If you block a port, you override all the service configurations.

You can block a port because:

- Blocked Ports protect your most sensitive services. The feature helps protect you from errors in your Firebox® configuration.
- Probes against sensitive services can make independent log entries.

With the default configuration, the Firebox blocks some destination ports. This gives a basic configuration that you usually do not have to change. It blocks TCP and UDP packets for these ports:

X Window System (ports 6000-6005)
: The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

X Font Server (port 7100)
: Many versions of X-Windows operate X Font Servers. The X Font Servers operate as the superuser on some hosts.

NFS (port 2049)
: NFS (Network File System) is a frequently used TCP/IP service where many users use the same files on a network. But, the new versions have important authentication and security problems. To supply NFS on the Internet can be very dangerous.

Note

The portmapper frequently uses the port 2049 for NFS. If you use NFS, make sure that NFS uses the port 2049 on all your systems.

rlogin, rsh, rcp (ports 513, 514)
: These services give remote access to other computers. They are a security risk and many attackers probe for these services.

RPC portmapper (port 111)
: The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are easy to attack through the Internet.

port 8000
: Many vendors use this port, and there are many security problems related to it.

port 1
: The TCPmux service uses Port 1, but not frequently. You can block it to make it more difficult for the tools that examine ports.

port 0
: This port is always blocked by the Firebox. You cannot add this port to the blocked ports list. You cannot allow traffic on port 0 through the Firebox.

Note

If you must allow traffic through for the types of software applications that use recommended blocked ports, we recommend that you allow the traffic only through an IPSec VPN tunnel or get access to the port using ssh for more security.

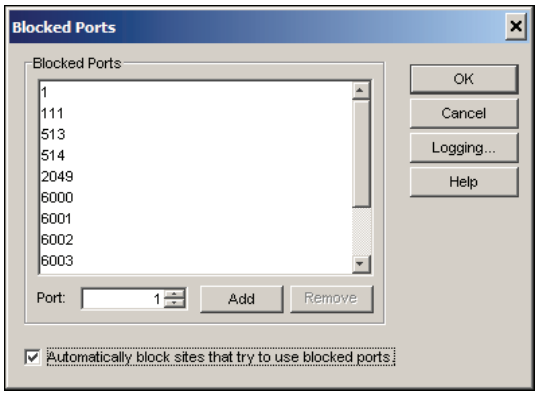
Avoiding problems with blocked ports

You can have a problem because of blocked ports. You must be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.

Blocking a port permanently

1 From Policy Manager, select **Setup > Intrusion Prevention > Blocked Ports**.
The Blocked Ports dialog box appears.

2 Type the port number. Click **Add**.
The new port number appears in the Blocked Ports list.



Automatically blocking IP addresses that try to use blocked ports

You can configure the Firebox to automatically block an external host that tries to get access to a blocked port. In the **Blocked Ports** dialog box, select the **Automatically block sites that try to use blocked ports** check box.

Setting logging and notification for blocked ports

You can configure the Firebox to make a log entry when a host tries to use a blocked port. You can also set up notification or set the Firebox to send an SNMP trap to an SNMP management server when a host tries to get access to a blocked port.

To set logging and notification parameters for blocked ports, use the same procedure as the one for blocked sites, as described in “Setting logging and notification parameters” on page 129.

CHAPTER 11

Using Signature-Based Security Services

Hackers use many methods to attack computers on the Internet. These attacks are created to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as intrusions.

WatchGuard® supplies the Gateway AntiVirus/Intrusion Prevention Service (GAV/IPS), which can identify and stop possible intrusions. The Intrusion Prevention Service operates with all WatchGuard proxies. WatchGuard Gateway AntiVirus operates with the SMTP proxy.

When a new intrusion attack is identified, the features that make the virus or attack unique are recorded. These recorded features are known as the signature. GAV/IPS uses these signatures to find viruses and intrusion attacks.

New viruses and intrusion methods appear on the Internet frequently. To make sure that GAV/IPS gives you the best protection, you must update the signatures frequently. You can configure the Firebox® to contact WatchGuard and update the signatures automatically. You can also update the signatures manually.

Note

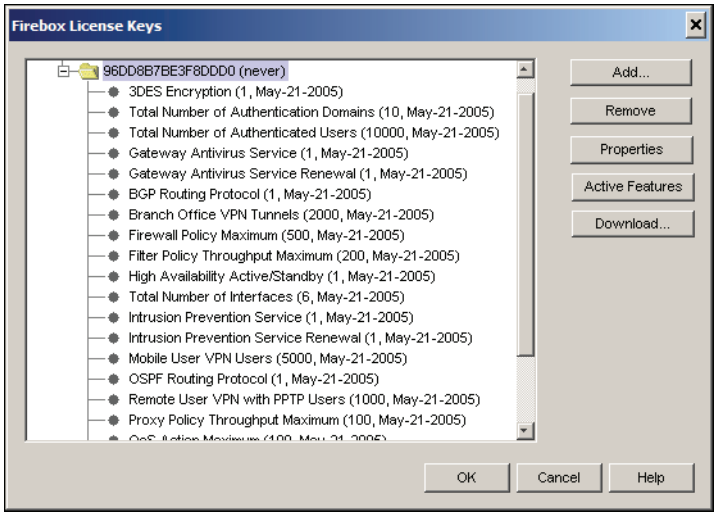
WatchGuard cannot guarantee that this product can stop all viruses or intrusions, or prevent damage to your systems or networks from a virus or intrusion attack.

Installing the Software Licenses

To install Gateway AntiVirus/Intrusion Prevention Service, you must have a GAV/IPS license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

To install this feature key:.

1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.


Firebox License Keys
96DD8B7BE3F8DDD0 (never)
3DES Encryption (1, May-21-2005)
Total Number of Authentication Domains (10, May-21-2005)
Total Number of Authenticated Users (10000, May-21-2005)
Gateway Antivirus Service (1, May-21-2005)
Gateway Antivirus Service Renewal (1, May-21-2005)
BGP Routing Protocol (1, May-21-2005)
Branch Office VPN Tunnels (2000, May-21-2005)
Firewall Policy Maximum (500, May-21-2005)
Filter Policy Throughput Maximum (200, May-21-2005)
High Availability Active/Standby (1, May-21-2005)
Total Number of Interfaces (6, May-21-2005)
Intrusion Prevention Service (1, May-21-2005)
Intrusion Prevention Service Renewal (1, May-21-2005)
Mobile User VPN Users (5000, May-21-2005)
OSPF Routing Protocol (1, May-21-2005)
Remote User VPN with PPTP Users (1000, May-21-2005)
Proxy Policy Throughput Maximum (100, May-21-2005)
Add...
Remove
Properties
Active Features
Download...
OK
Cancel
Help

2 Click **Remove** to remove the current feature key.

3 Click **Add**.

4 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

Activating Gateway AntiVirus

WatchGuard® Gateway AntiVirus (GAV) stops viruses before they get to computers on your network. GAV operates with the WatchGuard SMTP proxy. When you enable GAV, the SMTP proxy looks at e-mail messages and removes any viruses it finds.

Note

If your organization does not use an e-mail server protected by the Firebox®, Gateway AntiVirus does not protect against e-mail viruses.

Gateway AntiVirus finds viruses encoded with frequently used e-mail attachment methods. These include base64, binary, 7-bit, and 8-bit encoding. Gateway AntiVirus does not find viruses in unencoded or binhex-encoded messages; the Firebox® strips these types of messages.

Before you use Gateway AntiVirus in an SMTP proxy policy, you must use the Activate Gateway AntiVirus wizard to activate the feature and create a basic configuration. To do this:

1 From WatchGuard System Manager, select the Firebox that you want to use Gateway AntiVirus.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manger toolbar.

3 From Policy Manager, select **Tasks > Gateway AntiVirus > Activate**.
The Activate Gateway AntiVirus wizard starts.

4 Click **Next**.

5 Complete the wizard. The wizard has these screens:

Apply Gateway AntiVirus Settings to your policies

This screen includes a list of proxy policies that are already on your Firebox. From the list, select the proxy policies for which you want to enable Gateway AntiVirus. Any policies that have Gateway AntiVirus already enabled are not available.

Create proxy policies

This screen appears if your Firebox does not have policies created for SMTP.

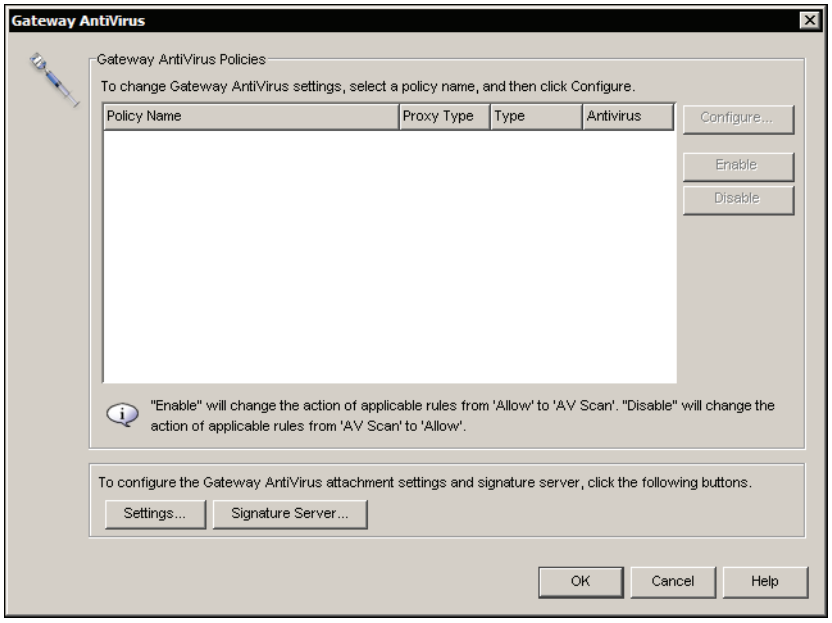
To create a policy, select the related check box. If you select SMTP, enter the e-mail server IP address.

This wizard creates a default SMTP policy, with static NAT enabled. To create this default SMTP policy, you must have a minimum of one external interface configured with a static IP address or PPPoE. You can have more than one external interface, but only one policy is created. The To field of the policy is a static NAT entry (the static IP address of the first external interface to the specified e-mail service IP address). If this default policy does not align with your requirements, you can create an SMTP policy in Policy Manager before you use this wizard.

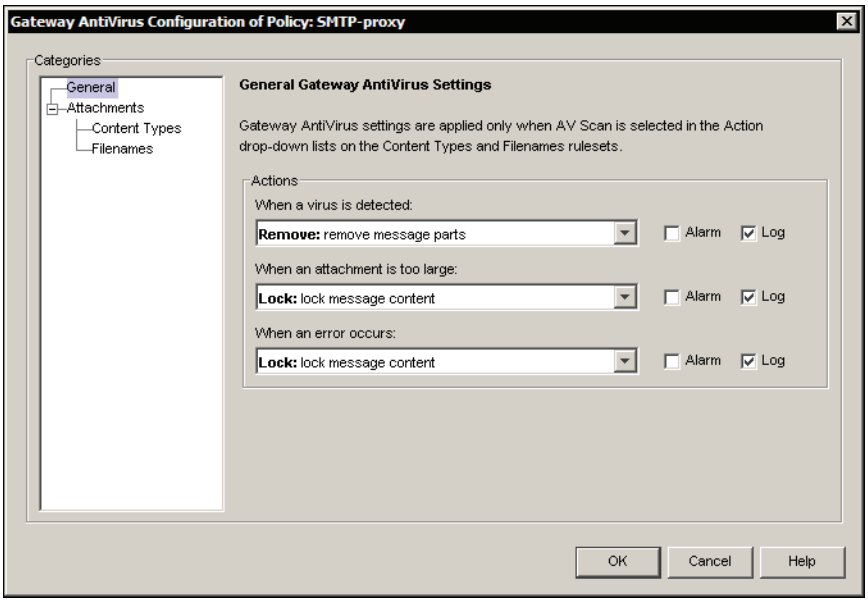
Configuring Gateway AntiVirus

After you use the Activate Gateway AntiVirus wizard to activate GAV and create a basic configuration, you can refine the configuration.

1 From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appear and shows the SMTP policies that have already been created.


Gateway AntiVirus
Gateway AntiVirus Policies
To change Gateway AntiVirus settings, select a policy name, and then click Configure.
Policy Name
Proxy Type
Type
Antivirus
Configure...
Enable
Disable
"Enable" will change the action of applicable rules from 'Allow' to 'AV Scan'. "Disable" will change the action of applicable rules from 'AV Scan' to 'Allow'.
To configure the Gateway AntiVirus attachment settings and signature server, click the following buttons.
Settings...
Signature Server...
OK
Cancel
Help

2 Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.



3 The fields on this dialog box set the actions necessary if a virus is found in an e-mail message. You also use this dialog box to set actions for when an e-mail message contains an attachment that is too large or that the Firebox® cannot scan. In the **Actions** section, use the drop-down lists to select the Firebox action for each of these conditions:

Allow
Allow the attachment to go to the recipient, even if the content contains a virus.

Lock
Lock the attachment. This is a good option for files that are too large for Gateway AntiVirus or that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment.

Deny
Deny the attachment and send a deny message to the sender.

Drop
Drop the attachment and drop the connection. No information is sent to the source of the message.

Block
Block the attachment, and add the IP address of the sender to the Blocked Sites list.

Note

If you set the configuration to allow attachments, your configuration is less secure.

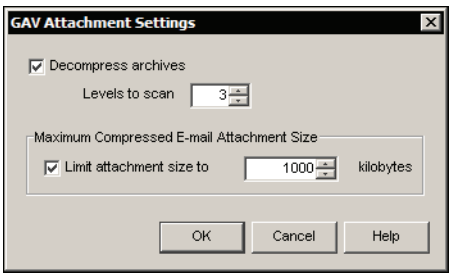
Creating alarms or log entries for antivirus responses

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the General Gateway Antivirus Settings page to create an alarm for an antivirus response. If you do not want an alarm for an antivirus response, clear the **Alarm** check box for that antivirus response.

If you want to record log messages for an antivirus response, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

Configuring GAV engine settings

1 From the **Gateway AntiVirus** dialog box, click **Settings**.

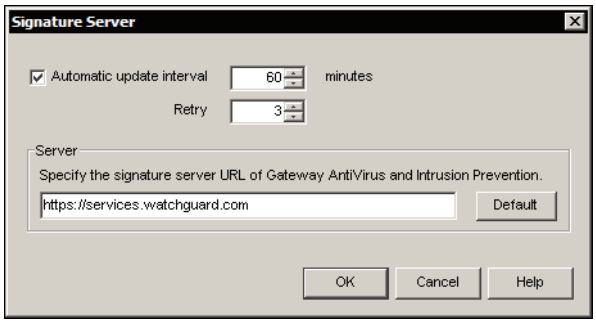


2 To scan inside compressed attachments, select the **Uncompress archives** check box. Select or type the number of compression levels to scan.
Compressed attachments that cannot be scanned include encrypted files or files that use a type of compression that we do not support such as a password-protected Zip files. Use the Gateway AntiVirus > Configure dialog box to set the action for the Firebox when it finds a message it cannot scan.

3 To limit the maximum file size for e-mail messages, select the check box and enter the maximum number of kilobytes.

Configuring the GAV signature server

1 From the **Gateway AntiVirus** dialog box, click **Signature Server**.



2 To enable automatic virus signature updates, select the **Automatic update** check box. Enter the number of minutes between automatic updates.

3 Select the number of tries if the automatic update fails.

4 It is usually not necessary to change the signature server URL. If you change this URL, GAV could fail. To change the URL to the default URL, click **Default**.

5 Click **OK**.

Using Gateway AntiVirus with more than one proxy

You can use more than one SMTP proxy to find and remove viruses for different servers in your organization.

Each proxy that uses Gateway AntiVirus is configured with options that are special to that proxy. For example, you can use different proxy antivirus configurations for e-mail that is for different servers or different destinations. You can strip attachments that are too large to scan for some users, and allow the same attachments for other users.

Unlocking an attachment locked by Gateway AntiVirus

WatchGuard® System Manager supplies an executable to unlock attachments locked by Gateway AntiVirus:

C:\Program Files\WatchGuard\wsm8\bin\unlock.exe

To open a locked file:

1 Open a command prompt.

2 Type: **Unlock** <path to locked file>

Getting Gateway AntiVirus Status and Updates

You can see the status and get updates for Gateway AntiVirus on the **Security Services** tab in Firebox® System Manager.

Seeing service status

Gateway AntiVirus status shows you if protection is active. You can also see information about the virus scanner, virus signature versions, and when the signatures were updated.

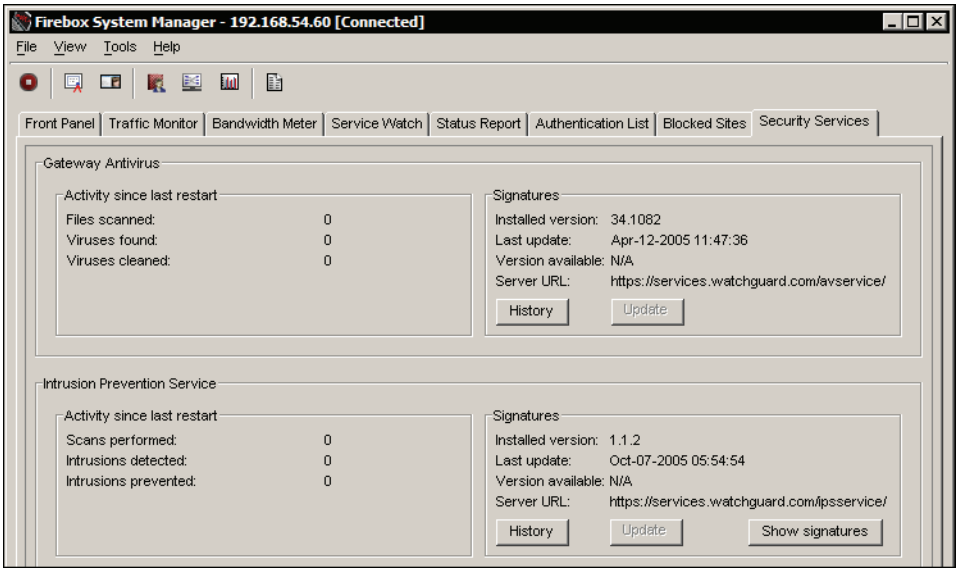
To see service status:

1 From WatchGuard® System Manager, select the Firebox. Select **Tools > Firebox System Manager**.

You can also click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

2 Click the **Security Services** tab.

The window shows the status of the installed security services. Licenses for these features must be installed to see status information.



Updating signatures manually

Gateway AntiVirus can be configured to update signatures automatically. You can also update signatures manually. If the signatures are not current, you are not protected from the latest viruses and attacks. To update the services manually:

1 Start Firebox System Manager.

2 Click the **Security Services** tab.

Security service status appears.

3 Click **Update** for the service you want to update. You must type your configuration passphrase.

The Firebox downloads the most recent available signature update for Gateway AntiVirus. You see information about the update in Traffic Monitor.

If no updates are available, the Update button is not active.

Updating the antivirus software

Because there are new types of attacks all the time, you must regularly update your antivirus software. When it is necessary, WatchGuard releases updates to the antivirus software. When we release an update, you get an e-mail from LiveSecurity. You have access to all updates while your Gateway Antivirus subscription is active.

To download software updates, log in to your LiveSecurity® account at:

www.watchguard.com/support

Activating Intrusion Prevention (IPS)

Hackers use many methods to attack computers on the Internet. They try to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as *intrusions*.

You use Intrusion Prevention Service to find and stop attacks with the WatchGuard® proxies. The Firebox® Intrusion Prevention Service examines DNS, FTP, HTTP, and SMTP traffic. It uses the TCP proxy to scan other TCP-based traffic.

Before you use IPS in a proxy policy, you must use the Activate Intrusion Prevention wizard to activate the feature and create a basic configuration. To do this:

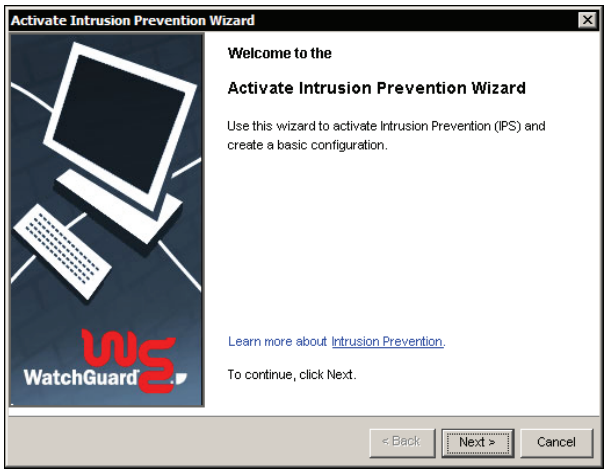
1 From WatchGuard System Manager, select the Firebox that will use IPS.

2 Select **Tools > Policy Manager**.

You can also click the Policy Manager icon on the WatchGuard System Manager toolbar.

3 From Policy Manager, select **Tasks > Intrusion Prevention > Activate**.

The Activate Intrusion Prevention wizard starts.


Activate Intrusion Prevention Wizard
Welcome to the
Activate Intrusion Prevention Wizard
Use this wizard to activate Intrusion Prevention (IPS) and create a basic configuration.
Learn more about Intrusion Prevention.
To continue, click Next.
WatchGuard
< Back
Next >
Cancel

4 Click **Next**.

5 Click through the wizard, which has these screens:

Select proxy policies to enable

This screen shows a list of proxy policies that are already specified on your Firebox. From the list, select the proxy policies you want to enable IPS for. Any policies that have IPS already enabled are shaded.

Create proxy policies

This screen shows the proxy types with corresponding policies that do not exist. If, for example, you have already created an SMTP policy, it does not appear in the list.

To create a policy, select the corresponding check box. If you select SMTP, enter the e-mail server IP address. This wizard creates a default SMTP policy, with static NAT enabled. To create this default SMTP policy, you must have one external interface configured with a static IP address or PPPoE. You can have more than one external interface, but only one policy is created. The To field of the policy is a static NAT entry (the static IP address of the first external interface to the specified mail service IP address). If this default policy does not align with your requirements, you can create an SMTP policy in Policy Manager before you use this wizard.

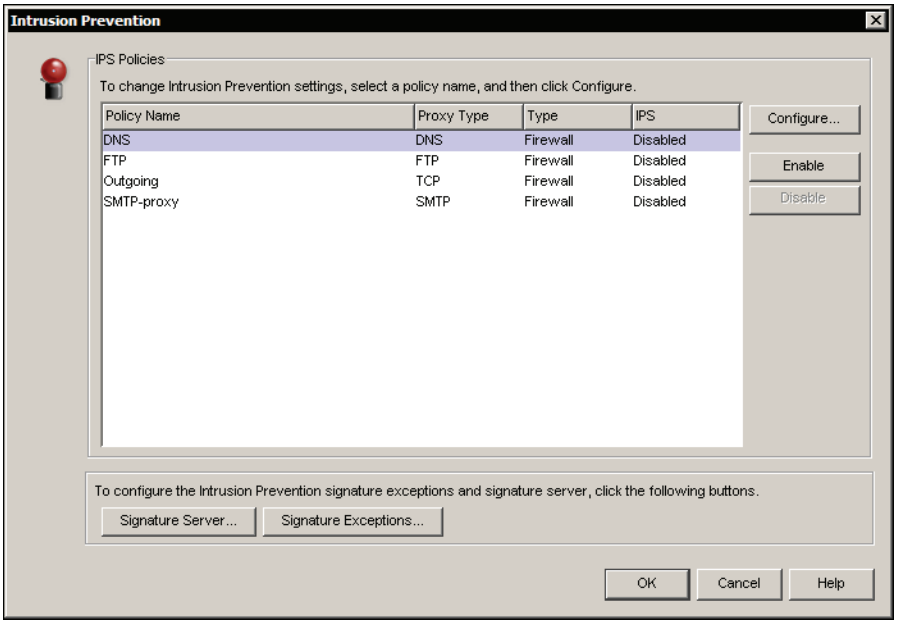
Select Advanced Intrusion Prevention settings (HTTP and TCP only)

If you use the wizard to add an HTTP or TCP policy, you can select protection against Instant Messaging (IM), Peer-to-Peer (P2P), and Spyware.

Configuring Intrusion Prevention

After you use the **Activate Intrusion Prevention** wizard to activate IPS and create a basic configuration, you can customize the configuration.

1 From Policy Manager, select **Tasks > Intrusion Prevention > Configure**.
The Intrusion Prevention dialog box appears and shows the policies that have already been created.



2 Select the policy you want to configure and click **Configure**.
The General Intrusion Prevention Settings page for that policy appears.

About intrusion severity levels

The proxy settings for intrusion prevention usually use three security levels. These three intrusion severity levels are:

High
: Vulnerabilities that allow remote access or execution of code, such as buffer overflows, remote command execution, password disclosure, backdoors, and security bypass.

Medium
: Vulnerabilities that allow access, show server-side source code to attackers, and deny access to legitimate users. Examples are directory traversal, file/source disclosure, DoS, SQL injection, and cross-site scripting.

Low
: Vulnerabilities that do not allow the attacker to directly get access, but allow the attacker to get information that can be used in an attack. For example, an attacker can send a command that gets information about the operating system, IP addresses, or topology of a network.

Signatures that get access to software applications with vulnerabilities (such as signatures that do not have very specific content) also get this level of severity.

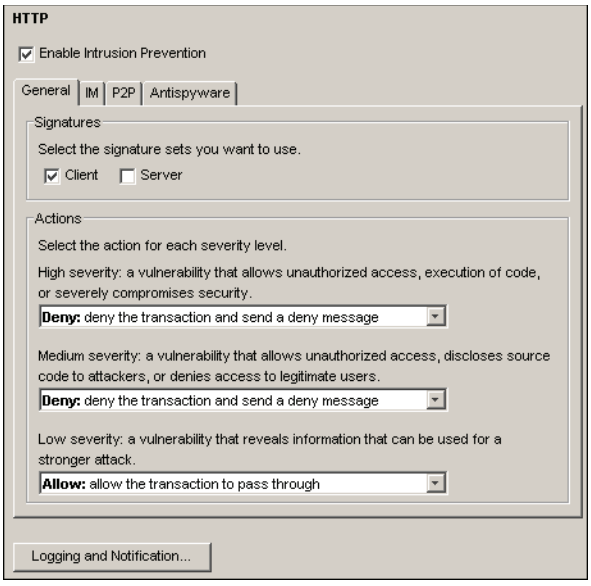
Some signatures that would usually be in the high or medium level are put in lower levels if their content is not very detailed. They are also put in lower levels if they have a wide scope that could cause false positives.

Configuring intrusion prevention for HTTP or TCP

The HTTP and TCP proxy include options to prevent Instant Messaging (IM), Peer to Peer (P2P), and spyware use.

If you use the TCP proxy and the HTTP proxy, you must be sure to configure actions for IM, P2P, and Spyware in the two proxies to apply actions to all IM, P2P, and Spyware traffic.

1 Select the **Enable Intrusion Prevention** check box.


HTTP
Enable Intrusion Prevention
General
IM
P2P
Antispyware
Signatures
Select the signature sets you want to use.
Client
Server
Actions
Select the action for each severity level.
High severity: a vulnerability that allows unauthorized access, execution of code, or severely compromises security.
Deny: deny the transaction and send a deny message
Medium severity: a vulnerability that allows unauthorized access, discloses source code to attackers, or denies access to legitimate users.
Deny: deny the transaction and send a deny message
Low severity: a vulnerability that reveals information that can be used for a stronger attack.
Allow: allow the transaction to pass through
Logging and Notification...

2 (HTTP only) Under **Signatures**, click one or both check boxes to use a more accurate list of signatures for HTTP client endpoints, HTTP server endpoints, or both.

3 In the **Actions** section, use the drop-down lists to select the Firebox® action for each severity level.

Allow
You allow a packet so it can get to its recipient, even if the content matches a signature.

Deny
You deny a packet to stop it and send a TCP reset packet to the sender.

Drop
You drop a packet to deny it, but send no TCP reset packet to the sender.

Block
You block a message to drop the packet, and to add the IP address that the packet started from to the Blocked Sites list.

Preventing Instant Messaging (IM) use

The HTTP Proxy has options to prevent Instant Messaging (IM) use. It finds these IM services:

- AOL Instant Messenger (AIM)
- ICQ
- MSN Messenger
- Yahoo Messenger

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **IM** tab.

2 Select the action to occur when the Firebox detects IM: **Allow**, **Drop**, **Deny**, or **Block**.

3 Select **IM Signature Categories** to enable sets of signatures for different IM services. You can then unselect services.

Preventing Peer to Peer (P2P) use

The HTTP Proxy has options to prevent Peer to Peer (P2P) use. It finds these types of P2P services:

- BitTorrent
- eDonkey2000 (ed2k)
- GNUtella
- Kazaa
- Napster
- Phatbot

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **P2P** tab.

2 Select the action to occur when the Firebox detects IM: **Allow**, **Drop**, **Deny**, or **Block**.

3 Select **P2P Signature Categories** to enable sets of signatures for different P2P services. You can then unselect services.

Blocking spyware

The HTTP and TCP proxies supply these antispyware categories:

Adware
: A software application in which advertising banners are shown while the program is in operation. It can include code that records a user's information and sends it to third parties, without the user's permission.

Dialer
: A software application that can hijack a user’s modem and dial toll numbers to get access to inappropriate web sites.

Downloader
: A program that gets and installs other files. Most are configured to get files from a designated web or FTP site.

Hijacker
: A type of malware program that changes your computer's browser settings and sends you to web sites that you did not plan to browse to.

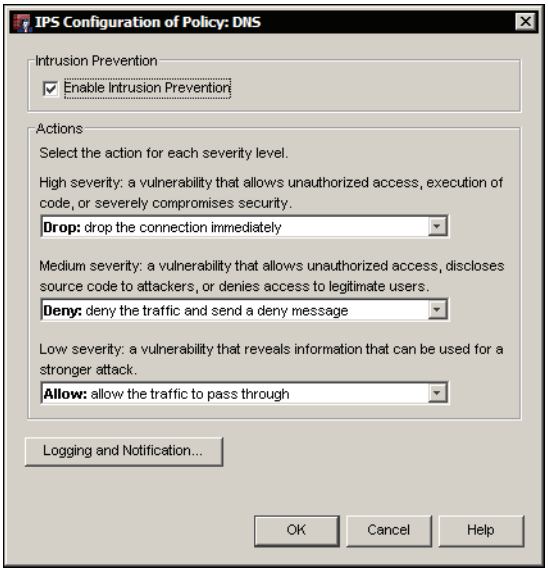
Trackware
Any software that uses a computer's Internet connection to silently send personal information without the user's permission.

1 From the Intrusion Prevention Services fields of the HTTP proxy, click the **Antispyware** tab.

2 Select the action to occur when the Firebox finds spyware: **Allow, Drop, Deny,** or **Block.**

Configuring Intrusion Prevention for FTP, SMTP, or DNS

1 Select the **Enable Intrusion Prevention** check box.


IPS Configuration of Policy: DNS
Intrusion Prevention
Enable Intrusion Prevention
Actions
Select the action for each severity level.
High severity: a vulnerability that allows unauthorized access, execution of code, or severely compromises security.
Drop: drop the connection immediately
Medium severity: a vulnerability that allows unauthorized access, discloses source code to attackers, or denies access to legitimate users.
Deny: deny the traffic and send a deny message
Low severity: a vulnerability that reveals information that can be used for a stronger attack.
Allow: allow the traffic to pass through
Logging and Notification...
OK
Cancel
Help

2 For each severity level, select one of the these actions.

Allow
Allow the attachment.

Deny
Deny the attachment and send a deny message to the sender.

Drop
Drop the attachment to stop the message and drop the connection. No information is sent to the source of the message.

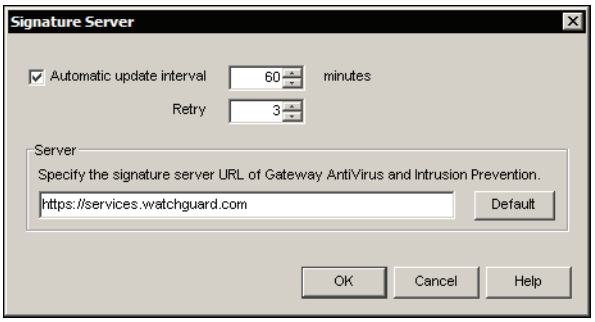
Block
Block a message to drop the attachment, and to add the IP address of the sender to the Blocked Sites list.

Note

If you set the configuration to allow attachments, your configuration is less secure.

Configuring the signature server

1 From the **Intrusion Prevention** dialog box, click **Signature Server**.



2 To enable automatic virus signature updates, select the **Automatic update** check box. Enter the number of minutes between automatic updates.

3 Select the number of retries if the automatic update fails.

4 It is usually not necessary to change the signature server URL. If you change this URL, IPS could fail. To change the URL to the default URL, click **Default**.

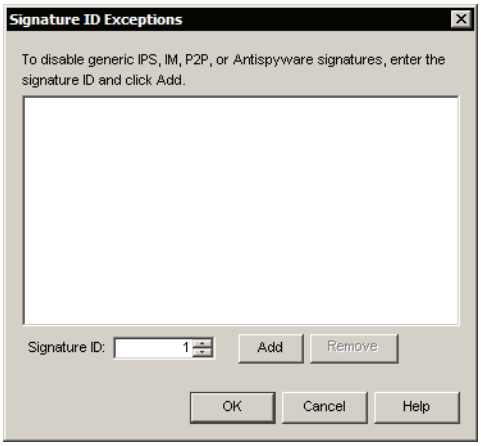
5 Click **OK**.

6 Select **File > Save > To Firebox**.

7 Type your configuration passphrase and click **OK**.

Configuring signature exceptions

1 From the **Intrusion Prevention** dialog box, click **Signature Exceptions**.
The Signature ID Exceptions dialog box appears.



2 Type any generic IPS, IM, P2P or Antispyware signatures that you want to disable. Click **Add**.

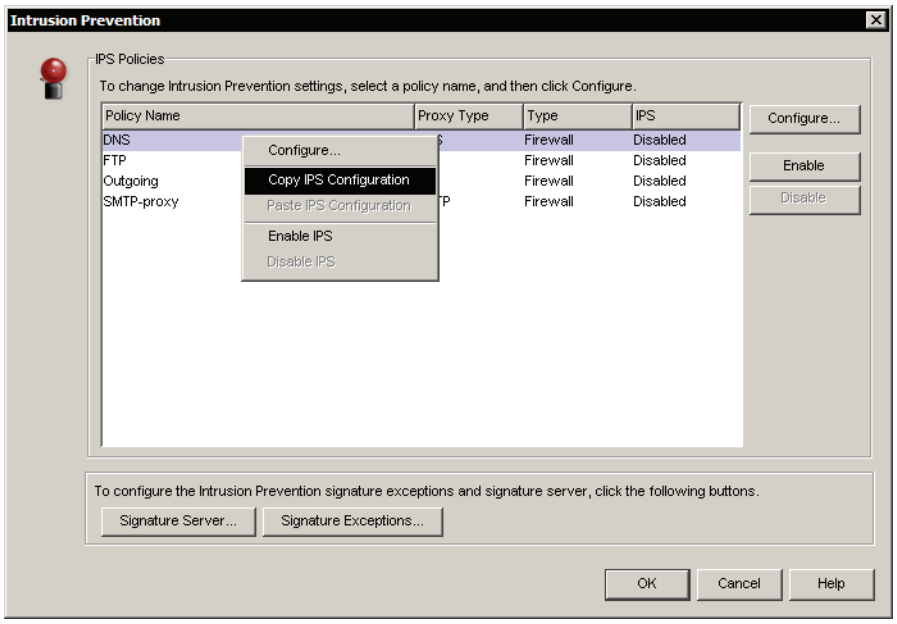
Copying IPS settings to other policies

After configuring IPS for one proxy, you can copy the same configuration to other proxies. You can copy IPS settings only between policies with compatible IPS configurations.

- Between FTP, DNS, and SMTP policies
- Between many TCP policies

- Between many HTTP policies

1 From the Intrusion Prevention dialog box, select the proxy with the configuration you want to copy, right-click, and select **Copy IPS Configuration**.



2 From the same dialog box, select the proxy or proxies you want to copy the configuration to, right-click, and select **Paste IPS Configuration.**

Getting Intrusion Prevention Service Status and Updates

You can see the status and get updates for Intrusion Prevention Service on the **Security Services** tab in Firebox® System Manager.

Seeing service status

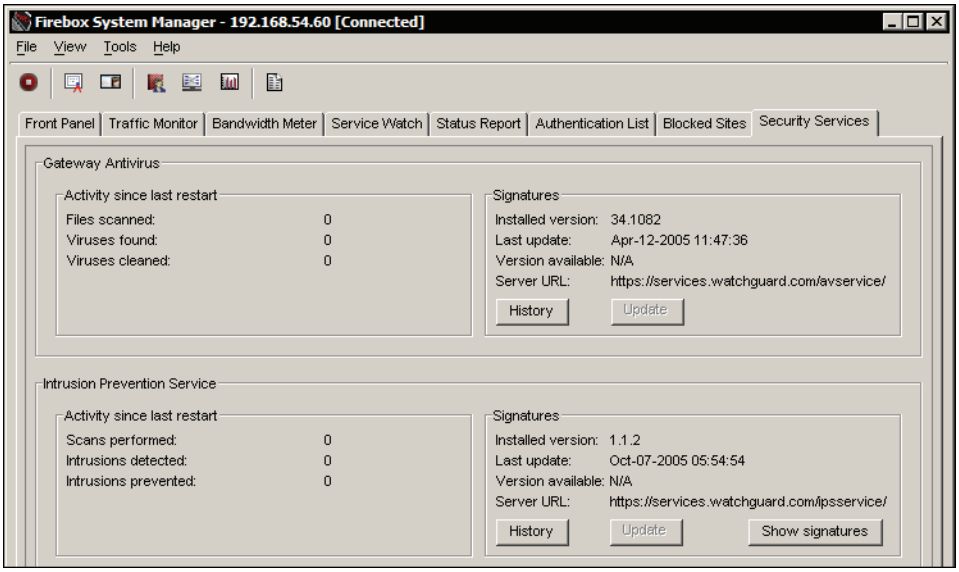
Intrusion Prevention Service status shows you if protection is active. You can also see information about the signature versions.

To see service status:

1 From WatchGuard® System Manager, select the Firebox. Select **Tools > Firebox System Manager**.

You can also click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

2 Click the **Security Services** tab.
The window shows the status for the installed security services. Licenses for these features must be installed to see status information.



3 Click **History** to see the date, version, and status of the signature updates that have occurred.

Updating signatures manually

Intrusion Prevention Service can be configured to update signatures automatically. You can also update signatures manually. If the signatures are not current, you are not protected from the latest viruses and attacks.

To update the services manually:

1 Start Firebox System Manager.

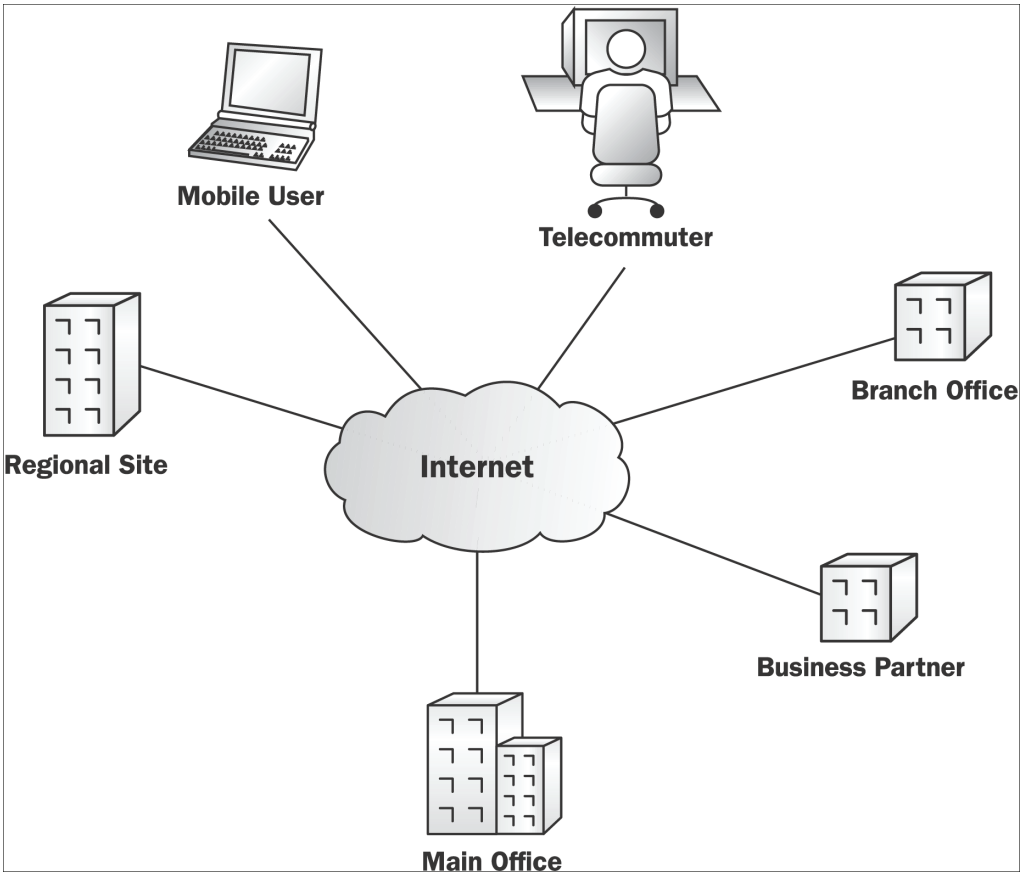
2 Click the **Security Services** tab.
Security service status appears.

3 Click **Update**.
The Firebox downloads the most recent available signature update. You see information about the update in Traffic Monitor.
If there are no updates available, the Update button is not active.

CHAPTER 12

Introduction to VPNs

The Internet is a public network. On this system of computers and networks, one computer can get information from other computers. It is possible for a person to read unsecured data packets that you send on the Internet. To send secure data on the Internet between offices, networks, and users, you must use stronger security.



Virtual private networks (VPNs) use encryption technology to decrease security risks, and to secure private information on the public Internet. A virtual private network lets data flow safely across the Internet between two networks. VPN tunnels can secure connections between a host and a network.

The networks and hosts at the endpoints of a VPN can be corporate headquarters, branch offices, and remote users.

VPN tunnels use authentication, which examines the sender and the recipient. If the authentication information is correct, the data is decrypted. Only the sender and the recipient of the message can read it clearly.

For more information on VPN technology, see the online information at:

http://www.watchguard.com/support

The WatchGuard® Support web site contains links to documentation, basic FAQs, advanced FAQs, and the WatchGuard User's Forum. You must log in to the Support web site to use some features.

Tunneling Protocols

Tunnels allow users to send data in secure packets across a network that is not secure, usually the Internet. A tunnel is a group of security protocols, encryption algorithms, and rules. The tunnel uses this information to send secure traffic from one endpoint to the other. A tunnel allows users to connect to resources and computers from other networks.

Tunneling protocols supply the infrastructure and set how the data transmission on the tunnel occurs. The two tunneling protocols that WatchGuard® uses are Internet Protocol Security (IPSec) and Point-to-Point-Tunneling Protocol (PPTP).

IPSec

You use the IPSec protocol to examine IP packets and make sure they are authenticated. IPSec includes security features including very strong authentication to protect the privacy of the information that you transmit on the Internet. IPSec is a standard that works with many systems from different manufacturers.

IPSec includes two protocols that protect data integrity and confidentiality. The AH (Authentication Header) protocol is the solution for data integrity. The ESP (Encapsulated Security Payload) protocol gives data integrity and confidentiality.

PPTP

Point to Point Tunneling Protocol (PPTP) is a standard for VPN security that can be used with many systems from different manufacturers. PPTP allows tunnels to corporate networks and to other PPTP-enabled systems. PPTP is not as secure as IPSec and cannot secure two networks. PPTP can only secure one IP address with one other IP address or with a network. PPTP supplies an inexpensive tunnel alternative for a corporate network that is easier to use than IPSec.

Encryption

On a network that is not secure, hackers can find transmitted packets very easily. VPN tunnels use encryption to keep this data secure.

The length of the encryption key, together with the algorithm used, set the encryption strength for the VPN. A longer key gives better encryption and more security. The level of encryption is set to give the

performance and security that is necessary for the organization. Stronger encryption usually gives a higher level of security, but can have a negative effect on performance.

Basic encryption allows sufficient security with good throughput for tunnels that do not transmit sensitive data. For administrative connections and for connections where privacy is very important, we recommend strong encryption.

The host or the IPSec device that sends a packet through the tunnel encrypts the packet. The recipient at the other end of the tunnel decrypts the packet. The two endpoints must agree on all the tunnel parameters. This includes the encryption and authentication algorithms, the hosts or networks allowed to send data across the tunnel, the time period for calculating a new key, and other parameters.

Selecting an encryption and data integrity method

Think of security and performance when you select the encryption and data integrity algorithms to use. We recommend Advanced Encryption Standard (AES), the strongest of the encryption types, for sensitive data. Fireware™ Pro uses AES 256 as the default encryption algorithm.

Data integrity makes sure that the data a VPN endpoint receives is not changed as it is sent. We give support to two types of data authentication. The first type is 128-bit Message Digest 5 (MD5-HMAC). The second type is 160-bit Secure Hash Algorithm (SHA1-HMAC).

Authentication

An important part of security for a VPN is to make sure that the sender and recipient are authenticated. There are two methods, passphrase authentication (also called a shared secret) and digital certificates. A shared secret is a passphrase that is the same for the two ends of the tunnel.

Digital certificates use public key cryptography to identify and authenticate the end gateways. You can use certificates for authentication for any VPN tunnel you create with your WatchGuard Management Server. For more information on the certificates, see the *WatchGuard System Manager User Guide*.

Extended authentication

Authentication for a remote user can occur through a database that is kept on the Firebox®, or through an external authentication server. An example of an external authentication server is the Remote Authentication Dial-In User Service (RADIUS). An authentication server is a safe third party that authenticates other systems on a network. With Mobile User VPN (MUVPN), which uses the IPSec tunneling protocol, the remote user must type a user name and password each time a VPN is started.

Selecting an authentication method

A primary part of a VPN is its method of user authentication. When you use shared secrets safely, you must make sure that you:

- Make users select strong passwords.
- Change passwords frequently.

When you use Remote User VPN (RUVPN), which uses the PPTP tunneling protocol, or MUVPN, it is very important to use strong passwords. When you put the security of VPN endpoints at risk, you can put the security of the network at risk. If, for example, a person steals a laptop computer and finds the password, that person has direct access to the network.

Digital certificates are electronic records that identify the user. For more information about certificates, see the *WatchGuard System Manager User Guide*. The Certificate Authority (CA), a safe third party, man-

ages the certificates. In the WatchGuard System Manager, you can configure a Firebox to operate as a CA. This type of authentication can be safer than shared secrets.

IP Addressing

Correct use of the IP address is important when you make a VPN tunnel. It is best if the private IP addresses of the computers at one side of the VPN tunnel are not the same as the private IP addresses you use at the other side of the VPN tunnel. If you have branch offices, use subnets at each location that are different from the primary office network. If it is possible, use subnets that are almost the same as the Firebox® subnet when you set up a branch office.

For example, if the primary Firebox network uses 192.168.100.0/24, then for the branch offices use 192.168.101.0/24, 192.168.102.0/24, and so on. This prevents new problems if you expand your network, and it helps you remember the IP addresses at your branch offices.

For MUVPN and RUVPN tunnels, the Firebox gives each remote user a virtual IP address. The easiest method is to give virtual IP addresses that come from the primary network but are not used for any other computer. You cannot use the same virtual IP address for RUVPN and for MUVPN remote users. You also cannot use a virtual IP address that can be on a computer at a different location on the primary network.

If your primary network does not have sufficient IP addresses to do this, the safest procedure is to install a "placeholder" secondary network. Select a range of addresses for it and use an IP address from that range for the virtual IP address.

This lets you select from a range of addresses. There is no interference from these addresses with real host addresses in use behind the Firebox. If you use this procedure for RUVPN virtual IP addresses, you must configure the client computer to use the default gateway on the remote network, or you must manually add routes after the VPN tunnel is connected. This is not necessary for the MUVPN client computer.

Internet Key Exchange (IKE)

As the number of VPN tunnels in your network increases, it can get more difficult to manage the large number of session keys that are used by the tunnels. Keys must be replaced frequently for stronger security.

Internet Key Exchange (IKE) is the key management protocol IPSec uses. IKE automates the procedure to negotiate and replace keys. The Internet Security Association and Key Management Protocol (ISAKMP) is a cryptographic protocol that is the basis of the IKE key interchange protocol. This protocol uses a two-phase procedure to create an IPSec tunnel. During Phase 1, two gateways create a safe, authenticated channel for VPN traffic. Phase 2 includes an interchange of keys to find out how to encrypt the data between the two.

Diffie-Hellman is an algorithm that IKE uses to make keys that are necessary for data encryption. Diffie-Hellman groups are collections of parameters. These groups let two peer systems interchange and agree on a session key. Group 1 is a 768-bit group, and group 2 is a 1024-bit group. Group 2 is more secure than group 1, but uses more processor time to make the keys.

Network Address Translation and VPNs

With Network address translation (NAT), the source and destination addresses of IP packets are changed as they go through the router or a firewall. If you use NAT between two VPN gateways, you must use ESP (not AH) as the authentication protocol when creating VPN tunnels between the devices.

If you send IPSec or PPTP traffic through a Firebox® (IPSec or PPTP pass-through), the Firebox can use NAT when sending the traffic.

Access Control

VPN tunnels lets users get access to resources on your computer network. Think which type of resources are needed by a given type of user. For example, you can let a group of contract employees get access to only one network and your sales personnel can get access to all the networks.

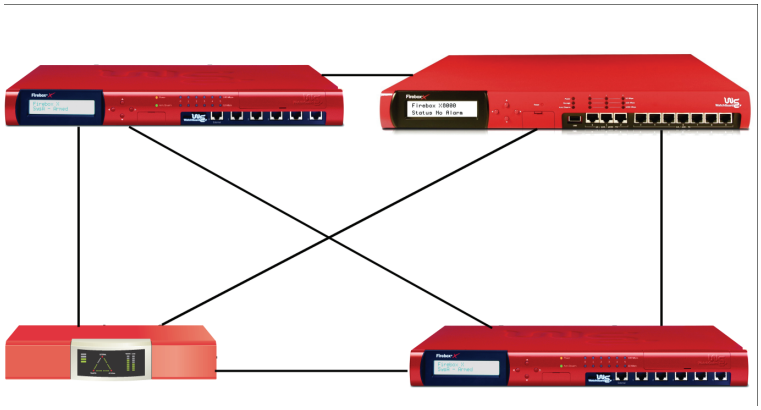
Different VPN types also can set your level of trust. Branch office VPNs (BOVPNs) have a firewall device at the two ends of the tunnel. They are more safe than MUVPN and RUVPN, which have protection at only one end.

Network Topology

You can configure the VPN for support of meshed and hub-and-spoke configurations. The topology that you select sets the types and number of connections that occur. It also sets the flow of data and the flow of traffic.

Meshed networks

In a fully meshed topology, all servers are connected together to make a web. Each device is only one step from each other VPN unit. Traffic can go between each unit of the VPN, if necessary.



Fully Meshed Network

This topology is the most error resistant. If a VPN unit goes down, only the connection to the trusted network of that unit is down. But, this topology is more work to set up. Each VPN unit must have a VPN tunnel configured to each other unit. There can be possible routing problems if it is not done carefully.

The largest problem that you get with fully meshed networks is one of control. Because each unit in the network must connect with each other unit, the number of necessary tunnels becomes large quickly.

The number of tunnels that are necessary for this configuration is the same as the square of the number of devices:

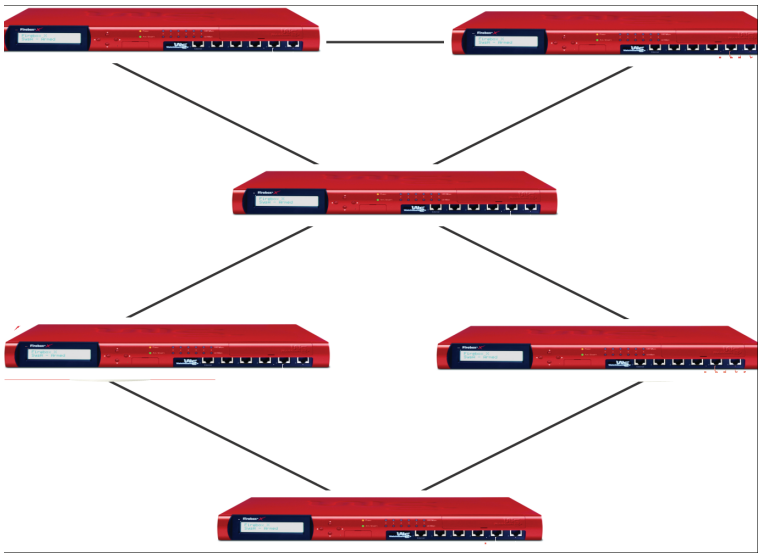
[(number of devices) x (number of devices)] -1 ÷ 2 = number of tunnels]

When all the VPN units are WatchGuard® devices, WatchGuard System Manager can make it easy to set up. The Management Server contains all the information for all the tunnels. With WatchGuard System Manager, you make a VPN tunnel between two devices in three steps using a drag-and-drop method.

You can monitor the security of the full system from more than one location, each with a Firebox®. Larger companies use this configuration with important branch offices, each using a higher capacity Firebox. Smaller offices and remote users connect with MUVPN, RUVPN, Firebox X Edge, or SOHO 6 devices.

Networks that are not fully meshed have only the necessary inter-spoke VPN tunnels. Refer to the figure below. Thus the flow through the network is better than fully meshed networks. The limits in all meshed networks are:

- The number of VPN tunnels that the firewall CPU can operate.
- The number of VPN tunnels allowed by the VPN license on the unit.



Partially Meshed Network

Hub-and-spoke networks

In a hub-and-spoke configuration, all VPN tunnels stop at one firewall. Smaller companies frequently use this configuration with a primary Firebox. Many distributed remote users connect with MUVPN, RUVPN, Firebox X Edge, or SOHO 6 devices to this configuration. Each remote device or remote user makes a VPN tunnel only to the primary Firebox.

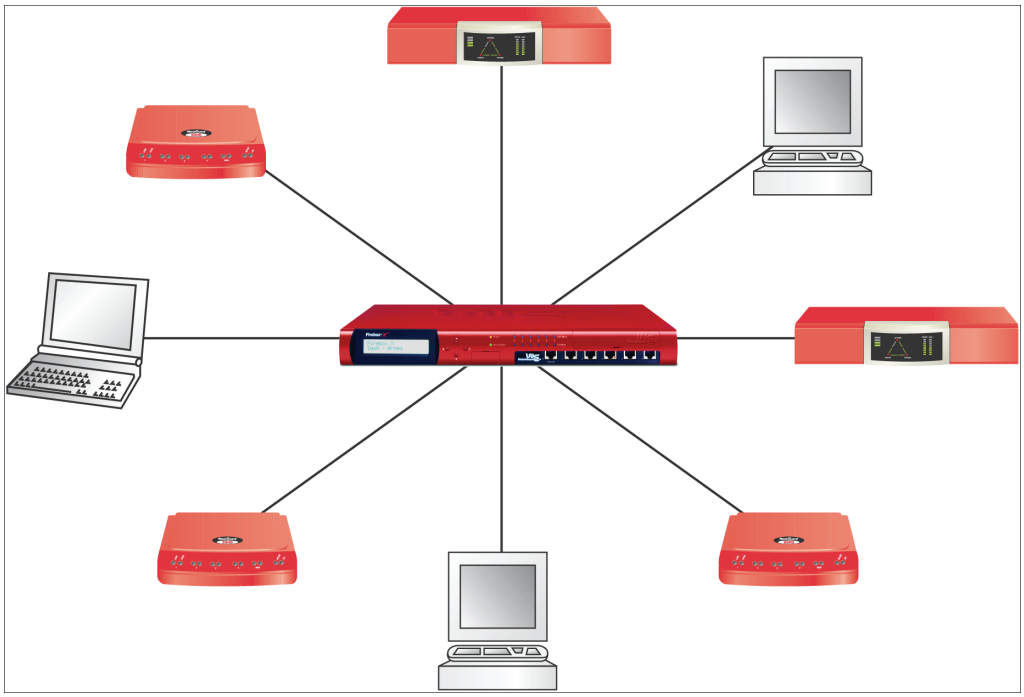
In a simple hub-and-spoke configuration, each remote location can send and receive data only through a VPN tunnel to the network behind the master server. A VPN tunnel to the master server, the primary hub, can also be configured to send and receive data to a different remote VPN location (tunnel switching). The intensity of traffic in hub-and-spoke can be high if the master server sends packets from one remote location to a different remote location. The traffic intensity also can be low in a simple hub-and-spoke, where the remote locations can only send data through a VPN tunnel to the primary hub location.

The master server is the one point where all VPN tunnels can fail, so it can be a problem. If the master server goes down, you cannot connect any VPN tunnels to the remote locations.

The flow through a simple hub-and-spoke system is far more clear than through a meshed system. You can control the number of tunnels better. Refer to the sum that follows:

[(number of devices) – 1 = number of tunnels]

If it is necessary to have more spoke capacity, you expand the hub location. But, because all traffic goes through the hub, it is necessary to have more bandwidth for this installation.



Hub and Spoke Network

Tunneling Methods

Split tunneling is when a remote user or endpoint has access to the Internet on the same computer as the VPN connection. But, this user does not put the Internet traffic through the tunnel. The remote user browses directly through the ISP. This makes the system vulnerable, because Internet traffic is not filtered or encrypted.

This dangerous configuration is less vulnerable when all of the Internet traffic of the remote user goes through a VPN tunnel to the Firebox®. From the Firebox, the traffic is then sent back out to the Internet (tunnel switching). With this configuration the Firebox examines all traffic and gives better security.

When you use tunnel switching, a Dynamic NAT policy must include the outgoing traffic from the remote network. This allows the remote users to browse the Internet when they send all traffic to the Firebox.

Split tunneling decreases security, but does increase performance. If you use split tunneling, remote users must have personal firewalls for computers behind the VPN endpoint.

WatchGuard VPN Solutions

WatchGuard® System Manager includes this software to create tunnels:

- Remote User VPN (RUVPN) with PPTP
- Mobile User VPN (MUVPN) with IPSec
- Branch Office VPN (BOVPN) with IPSec, which uses Policy Manager to manually configure the tunnel settings
- Branch Office VPN (BOVPN) with IPSec, which uses WatchGuard System Manager to automatically configure the tunnel settings.

WatchGuard includes different types of encryption for the different types of VPN tunnels you can create. BOVPN allows Data Encryption Service (DES) with a 56-bit encryption key for basic encryption, 112-bit key for moderate encryption, and a 168-bit encryption key (3DES) for strong encryption. It also allows the Advanced Encryption Standard (AES), a block data encryption method, using 128-bit, 192-bit, or 256-bit encryption.

Remote User VPN with PPTP

Remote User VPN allows remote users or mobile users to connect to the Firebox® network with PPTP. RUVPN with PPTP allows RC4 40-bit or 128-bit keys.

The basic WatchGuard System Manager package includes RUVPN with PPTP. It allows 50 users, and all levels of encryption. For information on how to create RUVPN with PPTP tunnels, see the chapter "Configuring RUVPN with PPTP," on page 175 in this guide.

Mobile User VPN

Note

For information on how to configure and use MUVPN, see the MUVPN Administrator Guide.

Mobile User VPN is an optional software component available for all Firebox models. Remote users are mobile employees who must have corporate network access. MUVPN creates an IPSec tunnel between a remote host that is not secure and your corporate network. Remote users connect to the Internet with a standard Internet dial-up or broadband connection, and then they use the MUVPN software to make a secure connection to the network or networks protected by the Firebox®. With MUVPN, only one Firebox is necessary to create the tunnel.

MUVPN uses IPSec with DES or 3DES to encrypt incoming traffic, and MD5 or SHA-1 to authenticate data packets. You configure a security policy and supply it along with the MUVPN software to each remote user. The security policy is an encrypted file with the extension wgx. When the software is installed on the computers of the remote users, they can safely connect to the corporate network. MUVPN users can change their security policies, or you can give them read-only security policies.

Branch Office Virtual Private Network (BOVPN)

Many companies have offices in more than one location. Offices frequently use data from other locations, or have access to shared databases.

Because branch offices have sensitive company data, information interchanges must be secure. When you use WatchGuard Branch Office VPN , you can connect two or more locations across the Internet without decreasing security. WatchGuard BOVPN supplies an encrypted tunnel between two networks

or between a Firebox and an IPSec-compliant device. You can use WatchGuard System Manager or Policy Manager to configure BOVPN.

WatchGuard allows certificate-based authentication for BOVPN tunnels. When you use certificate-based authentication for BOVPN, the two VPN endpoints must be WatchGuard Fireboxes. You cannot use certificate-based authentication for BOVPN with SOHO 6 or Firebox X Edge devices. To use this functionality, you must configure a Management Server and a certificate authority. For more information, see "Configuring Managed VPN Tunnels," on page 169. For instructions on how to use Policy Manager to manually configure a BOVPN tunnel, see "Configuring BOVPN with Manual IPSec," on page 161.

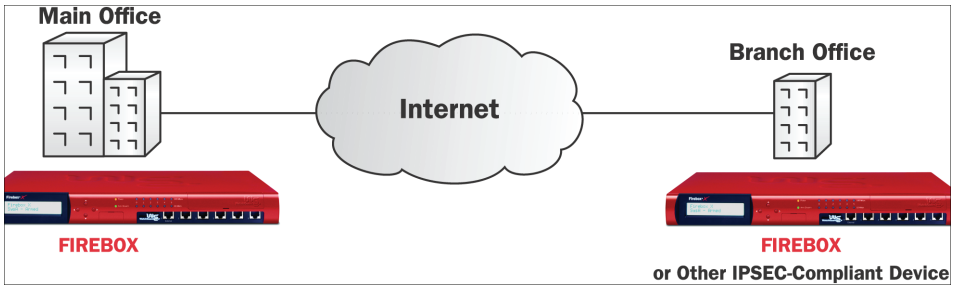
BOVPN with Policy Manager

When you make a tunnel with Policy Manager, the Firebox uses IPSec to make encrypted tunnels with a different IPSec-compliant security device. One of the two endpoints must have a public static IP address. Use BOVPN with Policy Manager if:

- You make tunnels between a Firebox and a non-WatchGuard, IPSec-compliant unit.
- You give different routing policies to different tunnels.
- Not all types of traffic go through the tunnel.

BOVPN with IPSec is available with the moderate encryption level of DES (56-bit), or the stronger encryption 3DES (168-bit). BOVPN is also available with AES at the 128-bit, 192-bit, and 256-bit encryption levels. AES with 256-bit encryption is the most secure.

You can create different VPN tunnels for different types of traffic on your network. For example, you can use a VPN tunnel with DES encryption for traffic from your sales team. At the same time use a VPN tunnel with stronger, 3DES encryption for all data from your finance department.



BOVPN with Manual IPSec

BOVPN with WatchGuard System Manager

With WatchGuard System Manager, you can make fully authenticated and encrypted IPSec tunnels with a drag-and-drop or menu interface. System Manager uses the Management Server to safely transmit IPSec VPN configuration information between Fireboxes. When you use the Management Server, you set each configuration parameter of the VPN. The Management Server keeps this information.

Use BOVPN with WatchGuard System Manager if:

- You make tunnels between two or more Fireboxes.
- You give different routing policies to different tunnels.
- Client units have dynamic or static IP addresses.
- You have a large number of tunnels to make.

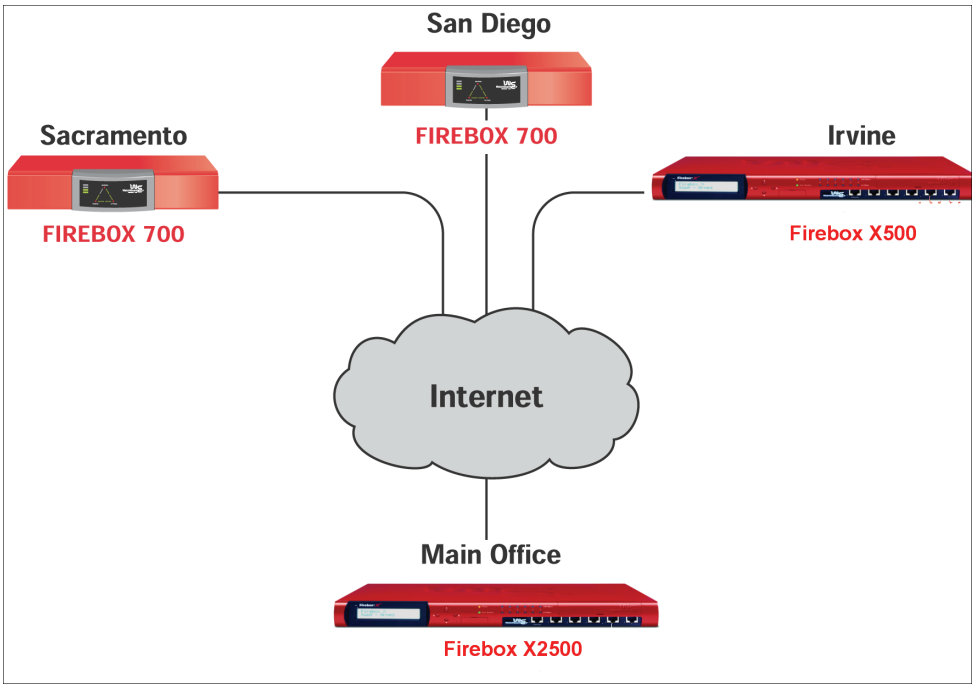
With WatchGuard System Manager you can configure, manage, and monitor all WatchGuard devices across a company. You can configure VPN tunnels between two remote devices easily, using the default

settings that System Manager gives you. You do not have to know about the Internet security of branch offices and remote users. Remote devices connect to the Management Server, and System Manager does all the work. If you use certificates for tunnel authentication, you can configure the Management Server as a certificate authority to create certificates automatically.

VPN Scenarios

This section gives three different types of companies and the VPN solutions that best fit each one.

Large company with branch offices: System Manager



Large Company with VPNs to Branch Offices

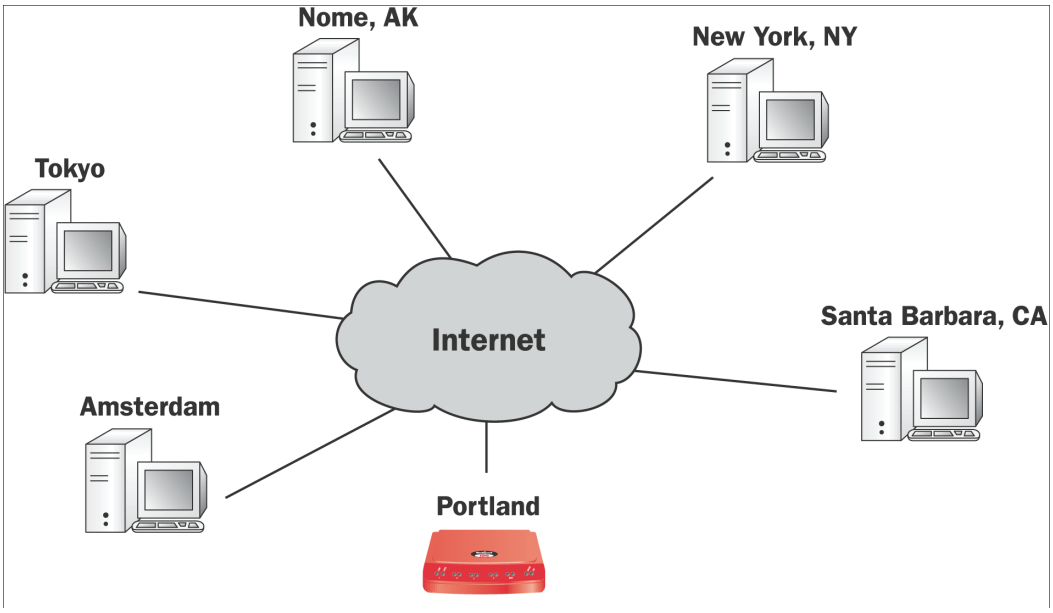
Gallatin Corporation has a head office with approximately 300 users in Los Angeles. It has branch offices of around 100 users each in Sacramento, San Diego, and Irvine. All locations have high-speed access to the Internet and employees at all locations must have secure connections to all other locations.

This company uses Fireboxes® at each location and WatchGuard® System Manager to connect the locations to each other. Each office connects to all other offices. All users at each office have access to the shared records at all the other locations. The Management Server is behind the Firebox at the primary office, and the Fireboxes at the branch offices are Managed Firebox Clients. When a service stop occurs with Gallatin's Internet service provider, it makes the Firebox at headquarters unavailable. But the tunnels in the other locations stay active.

Small company with telecommuters: MUVPN

River Rock Press is a small publishing company in a specialty market. It has an office with six employees in Portland, Oregon, and five editors who are in other locations. The head office uses a Firebox X Edge as

a firewall and as a VPN gateway. The five editors each use a MUVPN client to make a secure connection to the Information Center in Portland. The editors can always safely interchange information if their computers are connected to the Internet.



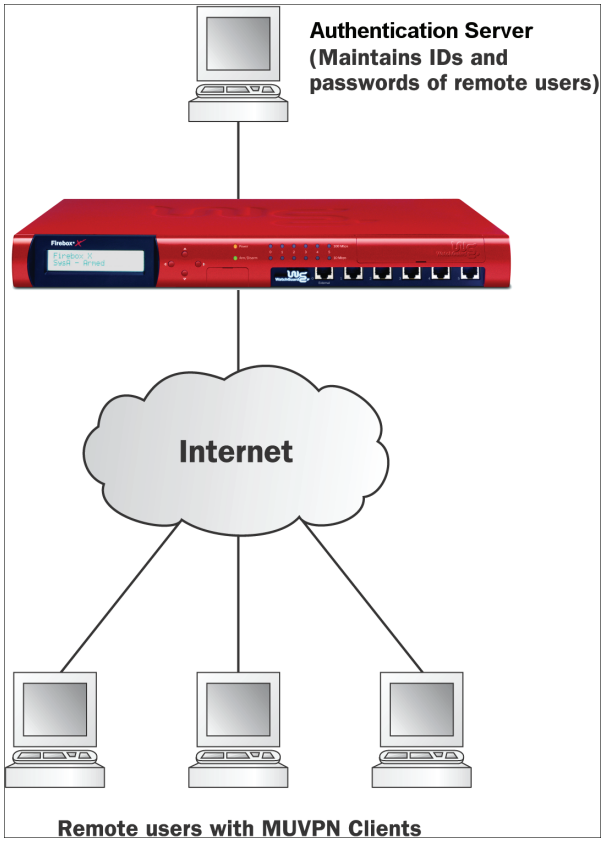
Small Company with Telecommuters Using Mobile User VPN

Company with remote employees: MUVPN with extended authentication

BizMentors, Inc. has 35 trainers to give classes on business topics at the locations of client companies. The 75 salespeople of BizMentors must have current information on the schedules of the trainers to prevent conflicts.

A database in the data center of BizMentors keeps this information current. The data center uses a Firebox and each salesperson uses an MUVPN client to get access to the inventory and price database. To authenticate all remote users, BizMentors uses a RADIUS authentication server.

Usually, you must enter the ID and password information on the Firebox and on the authentication server. But when you use extended authentication, all IDs and passwords are sent to the authentication server. You do not have to put them in the Firebox. All salespersons can log in to the corporate network with the ID and password they usually use when inside the network. The Firebox sends the ID and password to the authentication server, and the authentication server does the authentication of the VPN user credentials.



Small Company Using Extended Authentication

CHAPTER 13

Configuring BOVPN with Manual IPSec

You use Branch Office VPN (BOVPN) with Manual IPSec to make encrypted tunnels between a Firebox® and an IPSec-compliant security device. This device can protect a branch office or a different remote location. BOVPN with Manual IPSec is can use different encryption methods: DES (56-bit), 3DES (168-bit), AES 128, AES 192, and AES 256.

Before You Start

You must have the this information to use BOVPN with Manual IPSec:

- Policy endpoints — IP addresses of special hosts or networks that operate on the tunnel.
- Encryption method — the two ends of the tunnel must use the same encryption method.
- Authentication method — the two ends of the tunnel must use the same authentication method.

Configuring a Gateway

A gateway is a connection point for one or more tunnels. The connection method that the gateway uses to make a tunnel is the method you must use at the other end of the tunnel. The ISAKMP (Internet Security Association and Key Management Protocol), is one example.

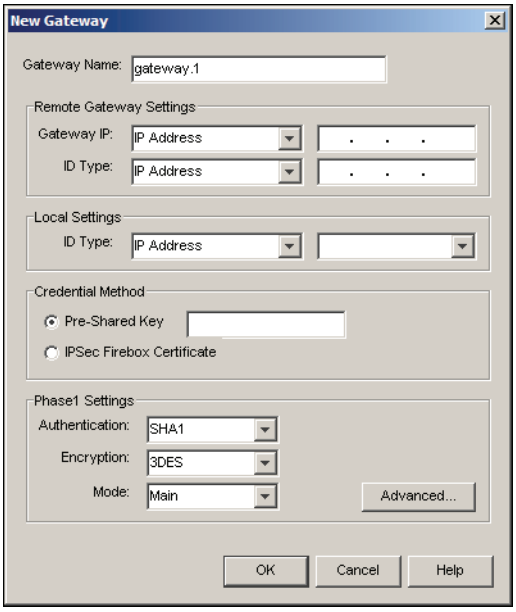
Adding a gateway

To start IPSec tunnel negotiation, one peer must connect to the other. You can use an IP address or a DNS name to connect the peers. If one peer has a dynamic IP address, select **Any** for the peer ID type.

To configure this, set the ID type of the remote gateway to **Domain Name**. Set the peer name to the fully qualified domain name. Set the DNS server of the Firebox® to one that can identify the name, usually an internal DNS server.

1 From Policy Manager, click **VPN > Branch Office Gateways**.
The Gateways dialog box appears.

2 To add a gateway, click **Add**.
The New Gateway dialog box appears.



3 In the **Gateway Name** text box, type the gateway name.
This name identifies the gateway only in Policy Manager.

4 From the **Gateway IP** drop-down list, select **IP Address** or **Any.**
If the gateway address is a static IP address, type it in the adjacent address box.

5 From the **Remote Gateway Settings ID Type** drop-down list, select **IP Address**, **Domain Name**, **User Domain Name**, or **X.500 Name**.
Use the domain name as the identification if the Firebox uses DHCP or PPPoE for its external IP address. This information is in the Firebox configuration. The Firebox uses IP Address and Domain Name to find the VPN endpoint. User name is a label that you use to identify the user at the VPN endpoint.

6 Configure the Local Settings. In the local **ID Type** drop-down list, select **IP address, Domain Name**, or **User Domain Name**. If you select **IP address**, you can select the IP address from the adjacent drop-down list. All configured Firebox interface IP addresses are shown.

7 Click **Pre-Shared Key** or **Firebox Certificate** to identify the authentication procedure to use. If you select **Pre-Shared Key**, type the shared key.
You must use the same shared key on the remote device.

Note

You must start the Certificate Authority if you select to authenticate with certificates. For information on this, see the Certificate Authority information in the *WatchGuard® System Manager User Guide*. Also, if you use certificates you must use the WatchGuard Log Server for log messages. We do not support third-party certificates.

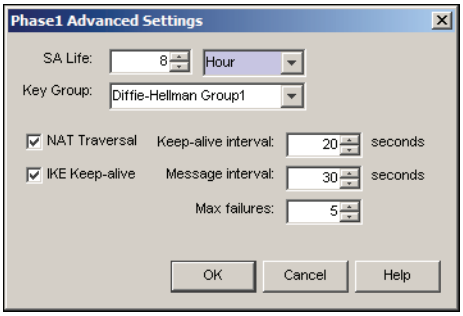
8 You can use the preconfigured Phase 1 settings, or you can change the settings.
Phase 1 applies to the initial phase of the IKE negotiation. It contains authentication, session negotiation, and key change information.

9 From the **Authentication** drop-down list, select **SHA1** or **MD5** as the type of authentication.

10 From the **Encryption** drop-down list, select **DES** or **3DES** as the type of encryption.

11 From the **Mode** drop-down list, select **Main** or **Aggressive**.
Main Mode does not identify the VPN endpoints during negotiation, and is more secure than Aggressive Mode. Main Mode also supports Diffie-Hellman group 2. Main Mode is slower than Aggressive Mode because Main Mode must send more messages between endpoints.

12 To change the Diffie-Hellman group settings and other advanced Phase 1 settings, click **Advanced**.
The Phase1 Advanced Settings dialog box appears.



13 To change the SA (security association) life, type a number in the **SA Life** field, and select **Hour** or **Minute** from the drop-down list.

14 From the **Key Group** drop-down list, select the Diffie-Hellman group you want. WatchGuard supports groups 1 and 2.
Diffie-Hellman refers to a mathmatic procedure to safely negotiate secret keys across a public medium. Diffie-Hellman groups are sets of properties that you use to get this. Group 2 is more safe than group 1, but uses more time to make the keys.

15 If you want to use NAT devices through the tunnel, select the **NAT Traversal** check box to enable NAT traversal. To set the **Keep-alive interval**, type the number of seconds or use the value control to select the number of seconds you want.
NAT Traversal, or UDP Encapsulation, allows traffic to get to the correct destinations. This continues to operate when the addresses are changed by NAT or when a router on the path between endpoints does not route IP 50 (ESP) or 51 (AH).

16 To have the Firebox send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box. To set the **Message Interval**, type the number of seconds or use the value control to select the number of seconds you want.

17 Use the field To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box. You can also use the value control to select the number of tries you want.

18 When you complete the advanced configuration, click **OK**.

19 Click **OK** to save the gateway.

20 Click **Close** to close the **Gateways** dialog box.

Editing and deleting a gateway

To change a gateway, select **VPN > Branch Office Gateways**. You can also right-click on a tunnel icon in the **BOVPN** tab of Policy Manager, and select **Gateway Property**.

1 Select the gateway you want and click **Edit**.
The Edit Gateway dialog box appears.

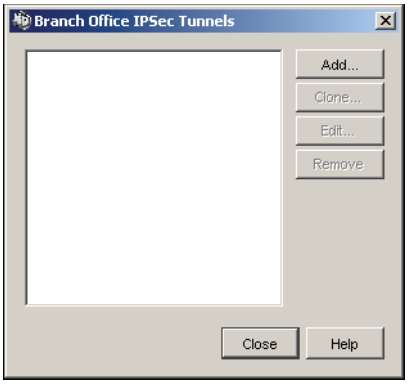
2 Make the changes and click **OK**.

To remove a gateway from the **Gateways** dialog box, select the gateway and click **Remove**.

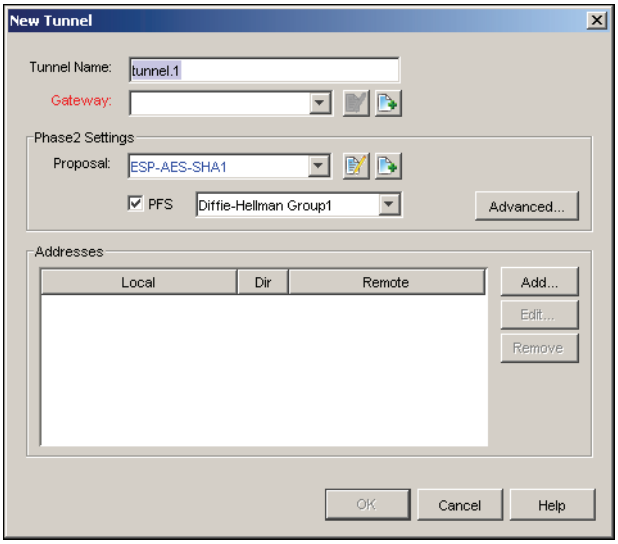
Making a Manual Tunnel

Use this method to configure a manual tunnel that uses a gateway with the ISAKMP (Internet Security Association and Key Management Protocol) key negotiation type. ISAKMP is a protocol that authenticates network traffic between two devices. This procedure includes the information on how the devices control security, which includes encryption. It also includes how to make the keys that you use to change the encrypted data into text.

1 From Policy Manager, select **VPN > Branch Office Tunnels**.
The Branch Office IPSec Tunnels dialog box appears.



2 Click **Add**.
The New Tunnel dialog box appears.



3 In the **Tunnel Name** box, type the tunnel name you want.

4 From the **Gateway** drop-down list, select a remote gateway to connect with this tunnel. The gateways you add to your configuration appear in this drop-down list.
To edit a gateway, select the name and click the Edit button. To create a new Gateway, click the New button.

Edit

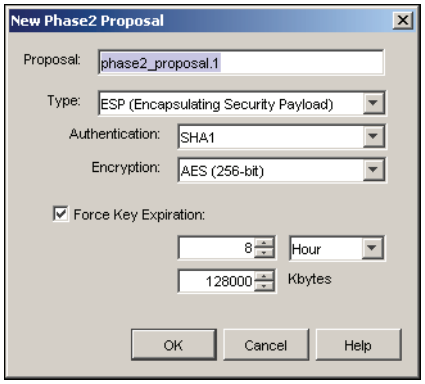
New

5 From the **Proposal** drop-down list, select the IKE Phase 2 proposal for your tunnel. The drop-down list contains predefined phase 2 security proposals.

6 If you want to use a predefined phase 2 proposal, and not create or edit a phase 2 proposal, go to Step 13.

You can edit any phase 2 proposal that you create, but you cannot edit a predefined proposal. You must add a new one. To edit a phase 2 proposal that you create, select the proposal name and click the **Edit** button. To create a new proposal, click the **New** button.

The Phase2 Proposal dialog box appears.



7 Type a name for the new proposal.

8 From the **Type** drop-down list, select **ESP** or **AH** as the proposal method.
ESP is authentication with encryption. AH is authentication only. Also, ESP authentication does not include the IP header, while AH does. The use of AH is rare.

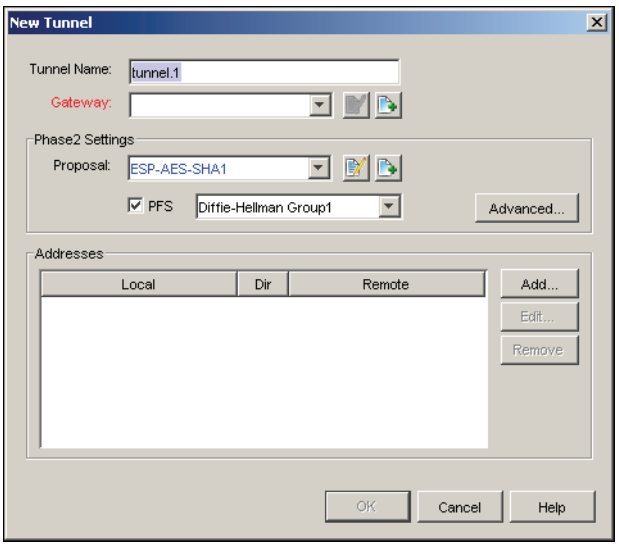
9 From the **Authentication** drop-down list, select **SHA1**, **MD5**, or **None** for the authentication method.

10 (ESP only) From the **Encryption** drop-down list, select the encryption method.
The options are DES, 3DES, and AES 128, 192, or 256 bit which appear in the list from the most simple and least secure to most complex and most secure.

11 You can make the key expire after a quantity of time or a quantity of traffic. To enable key expiration, select the **Force Key Expiration** check box.

12 Select a quantity of time and a number of bytes after which the key expires. The key expires when the time selected or the number of bytes occurs.

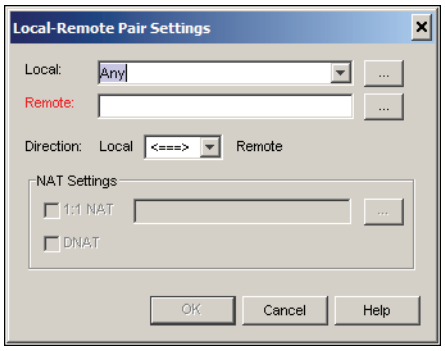
13 Click **OK** to close the **Phase2 Proposal** dialog box.



14 Select the **PFS** check box to enable Perfect Forward Secrecy (PFS). If you enable PFS, select the Diffie-Hellman group.
Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure. Diffie-Hellman Group 1 uses a 768-bit group to create the new key exchange, and Diffie-Hellman Group 2 uses a 1024-bit group.

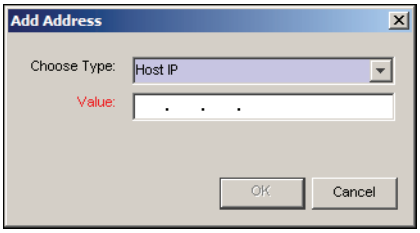
15 Click **Advanced** to configure advanced settings. Use the **Phase2 Advanced Settings** dialog box to configure the tunnel to use Any for the policy or for the address. Click **OK** when you are done.
If "Use Any for Service" is not selected, a security association (SA) is created for each set of port/protocol pairs defined in each policy that is used. This creates a different VPN tunnel for each policy. If "Use Any for Address" is not selected, a security association (SA) is created based on the tunnel routes (the local-remote pairs).

16 In the **New Tunnel** dialog box in the **Addresses** block, click **Add** to add a pair of addresses that use the tunnel.
The Local-Remote Pair Settings dialog box appears.



17 From the **Local** drop-down list, select the local address you want.
You can also click the button adjacent to the Local drop-down list to use an IP address, network address, or a range of IP addresses.

18 In the **Remote** box, type the remote network address. Click the button adjacent to the **Remote** box to open the **Add Address** dialog box.



19 From the **Choose Type** drop-down list, select the type of address you want to use.
Select **Host IP** (one IP address), **Network IP** (a network IP address with the mask in slash notation), or **Host Range** (a range of IP addresses).

20 In the **Value** text box, type an IP address or network address.

21 Click **OK**.
The Add Address dialog box closes. The Local-Remote Pair Settings dialog box reappears.

22 From the Direction drop-down list, select the direction for tunnel. The tunnel direction decides which end of the VPN tunnel can start a VPN connection through the tunnel.

23 You can enable NAT for the tunnel. Select the **1:1 NAT** check box or the **DNAT** check box.
The options that you can select for NAT are different for different types of addresses and different tunnel directions. For 1:1 NAT, type the address to change with NAT in the field.
Dynamic NAT is also available through the VPN. You must set a unidirectional tunnel from LAN1 to LAN2 where you want all LAN1 to connect to LAN2 servers but only appear as one IP address on LAN2. You must then enable Dynamic NAT in the phase 2 settings of the LAN2 Firebox.

24 After you configure the pair, click **OK**.

25 When you complete tunnel configuration, click **OK**.

Editing and deleting a tunnel

To change a tunnel, select **VPN > Branch Office Tunnels**. You can also right-click on a tunnel icon in the **Branch Office VPN** tab of Policy Manager, and select **Tunnel Property**.

1 Select the tunnel and click **Edit**.
The Edit Tunnel dialog box appears.

2 Make the changes and click **OK**.

To delete a tunnel from the **Branch Office IPSec Tunnels** dialog box, select the tunnel and click **Remove**.

Making a Tunnel Policy

Tunnel policies are sets of rules that apply to tunnel connections.

The default configuration includes the "Any" policy. This allows all traffic to use the tunnel. You can delete this policy. Then, create a custom VPN policy to select the ports you allow or to use a proxy for the traffic.

1 From Policy Manager, click the **Branch Office VPN** tab.

2 From the **Show** menu, select the tunnel to which you want to add policies.

3 Right-click in Policy Manager and select **New Policy.**
If you have not selected a BOVPN tunnel from the Show menu, a dialog box appears with a prompt for you to select a tunnel. Select the tunnel and click OK.

4 Configure policies. For more information, see "Creating Policies for your Network" on page 63.
Address information for BOVPN policies is different from standard Firebox policies. You configure the addresses with the Local-Remote Pairs dialog box.

Allow VPN connections for specified policies

To let traffic through from VPN connections only for specified policies, add and configure each policy. It can be necessary to delete the "Any" policy to create the necessary restrictions.

CHAPTER 14

Configuring Managed VPN Tunnels

WatchGuard® System Manager supplies speed and reliability when you create IPSec VPN tunnels through drag-and-drop tunnels, an automatic wizard, and the use of templates. You can make IPSec tunnels that use authentication and encryption in minutes. You can be sure that these tunnels operate with other tunnels and security policies.

From the same interface, you can control and monitor the VPN tunnels. For more information on how to monitor tunnels, see "Monitoring Your Network" in the *WatchGuard System Manager User Guide*.

WatchGuard System Manager also allows you to safely manage Firebox® X Edge devices from a remote location. For more information, see "Managing the Firebox X Edge and Firebox SOHO 6" in the *WatchGuard System Manager User Guide*.

Steps in making VPNs

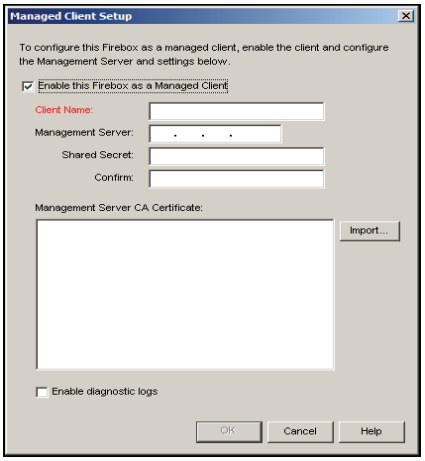
- Configure a WatchGuard Management Server and Certificate Authority (CA)
- Add Fireboxes or Firebox X Edge or SOHO devices to the Management Server
- (Dynamic devices only) Configure the Firebox as a Managed Client
- Make policy templates to configure which networks can connect through VPN tunnels
- Make security templates to set the encryption type and authentication type
- Make tunnels between the devices

Configuring a Firebox as a Managed Firebox Client

To allow WatchGuard® System Manager to manage a Firebox®, Edge, or SOHO with a dynamic IP address, you must enable it as a managed Firebox client. The instructions here give you the steps to configure a Firebox III or Firebox X as a managed Firebox client. To configure a Firebox X Edge or Firebox SOHO as a managed Firebox client, refer to your Edge or SOHO User Guide for information about using the device with managed VPN.

1 Make sure that the Management Server is configured and that you added the required devices. For more information, see the "Configuring and Using the Management Server" chapter.

2 From Policy Manager, select **VPN > Managed Client**.
The Managed Client Setup dialog box appears.



3 To set up a Firebox as a managed device, select the **Enable this Firebox as a Managed Client** check box.

4 In the **Client Name** box, type the name you want to give the Firebox.

5 To enable the managed client to send log messages to the log server, select the **Enable diagnostic logs** check box. (We recommend this option only to perform troubleshooting).

6 In the **Management Server** address box, type the IP address of the Management Server.

7 In the **Shared Secret** box, type the shared secret.

8 Click **OK**.

9 Start the Firebox again.
The Firebox connects to the Management Server.

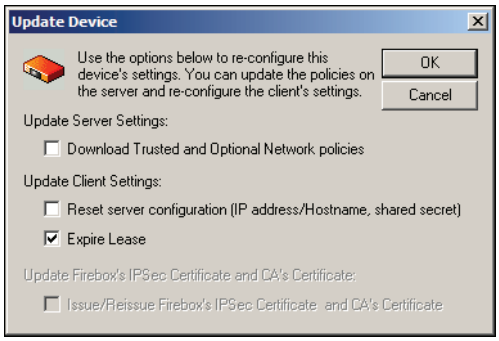
Adding Policy Templates

For a VPN, you can configure (and put a limit to) the networks that have access through the tunnel. You can make a VPN between two hosts or between more networks. To configure the networks that are available through a given VPN device, you make policy templates. By default, WatchGuard® System Manager (WSM) adds and applies a network policy template that gives access to the network behind the VPN device, if the device has a static IP address.

Get the current templates from a device

Before you add more policy templates, get the current templates from the device. This is most important for dynamic devices because the Firebox® automatically adds a network policy template for static devices Before you update a device, make sure that it is configured as a managed Firebox client.

1 In WatchGuard System Manager on the **Device Management** tab, select a managed client, and then click **Edit > Update Device**.
The Update Device dialog box appears.


Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

2 Select the **Download Trusted and Optional Network Policies** check box.

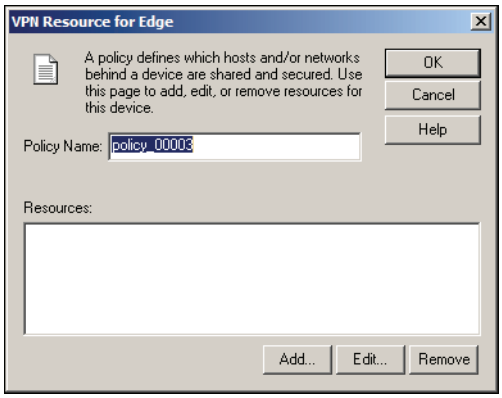
3 Click **OK**.

Make a new policy template

To make a policy template, on the **Device Management** tab:

1 Select the device for which you want to configure a policy template.

2 Right-click and select **Insert VPN Resource** or click the Insert VPN Resource icon.
The VPN Resource dialog box for that device appears.



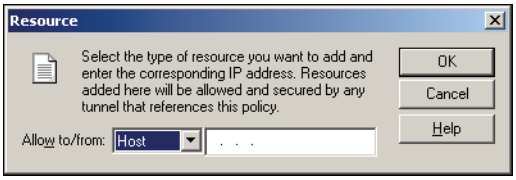
3 In the **Policy Name** box, type the policy name you want.

4 Add, edit, or delete resources from the tunnel policy. Click **Add** to add an IP address or a network address to the tunnel policy. Click **Edit** to edit a resource that you have selected in the list. Select a resource in the **Resources** list and click **Remove** to delete a resource.

5 Click **OK**.
The policy template is configured and is available in the VPN configuration area.

Adding resources to a policy template

1 From the **VPN Resource** dialog box, click **Add**.
The Resource dialog box appears.


Resource
Select the type of resource you want to add and enter the corresponding IP address. Resources added here will be allowed and secured by any tunnel that references this policy.
OK
Cancel
Help
Allow to/from:
Host

2 From the **Allow to/from** drop-down list, select the resource type, and then type the IP address or network address in the adjacent address box.

3 Click **OK**.

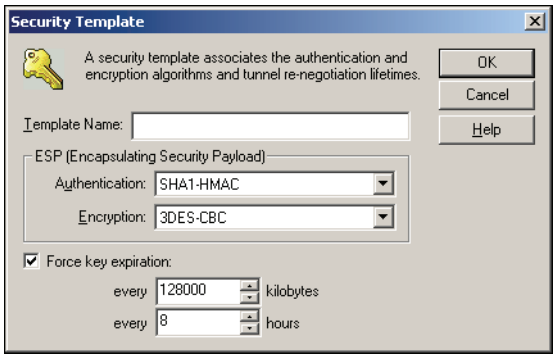
Adding Security Templates

A security template gives the encryption type and authentication type for a tunnel.

Default security templates are supplied for the available encryption types. You can also make new templates. Security templates make it easy to set the encryption type and authentication type with the tunnel from the Configuration Wizard.

To make a policy template, on the **Device Management** tab:

1 Right-click in the window, and select **Insert Security Template** or click the Insert Security Template icon (shown at the left side).
The Security Template dialog box appears.



2 In the **Template Name** box, type the template name you want to use. From the **Authentication** and **Encryption** drop-down lists, select the authentication method and encryption method.

3 To set the end date for a key, select the **Force key expiration** check box, and then select the kilobytes or hours until the expiration.
If you give two values, the key stops at the event that comes first.

The security template is configured. You can select it in the VPN Wizard when you make a VPN tunnel with that device.

4 Click **OK**.

Making Tunnels Between Devices

You can configure a tunnel with the drag-and-drop procedure or the Add VPN wizard.

Using the drag-and-drop procedure

To use the drag-and-drop tunnel procedure, dynamic Fireboxes and Firebox® X Edge or SOHO devices must have networks that are configured before you can use this procedure. You must also get the policies from any new dynamic devices before you configure drag-and-drop tunnels (use the procedure "Get the current templates from a device" on page 171 to do this).

On the **Device Management** tab:

1 On one of the tunnel endpoints, click the device name. Drag-and-drop name to the device name at the other tunnel endpoint.
The Add VPN wizard starts.

2 Click **Next**.

3 The gateway devices screen shows the two endpoint devices you selected with drag-and-drop, and the policy templates that the tunnel uses. If the endpoints are not shown, select them on this screen.

4 From the drop-down list, select a policy template for each device.
The policy template configures the resources available through the tunnel. Resources can be a network or a host. The drop-down list shows the policy templates that you added to WatchGuard System Manager.

5 Click **Next**.
The wizard shows the Security Policy dialog box.

6 Select the security template applicable for the type of security and type of authentication to use for this tunnel.
The list shows the templates you added to the Management server.

7 Click **Next**.
The wizard shows the configuration.

8 Select the **Restart devices now to download VPN configuration** check box. Click **Finish** to start the devices again and deploy the VPN tunnel.

Using the Add VPN wizard without drag-and-drop

To create tunnels using the Add VPN wizard without drag-and-drop:

1 From the **Device Management** tab, select **Edit > Create a new VPN** or click the Create New VPN icon.
This starts the Add VPN wizard.

2 Click **Next**.
The wizard shows two lists that each show all the devices registered in the Management Server.

3 Select a device from each list box to be the endpoints of the tunnel you make.

4 Select the policy templates for the end of the tunnel of each device.
The list shows the templates added to the Management Server.

5 Click **Next**.
The wizard shows the Security Template dialog box.

6 Select the applicable security template for this VPN and click **Next**.
The wizard shows the configuration.

7 Select the **Restart devices now to download VPN configuration** check box. Click **Finish** to start the devices again and deploy the VPN tunnel.

Editing a Tunnel

You can see all your tunnels on the **Device Management** tab of WatchGuard® System Manager (WSM). WSM lets you change the tunnel name, security template, endpoints, and the policy you use.

On the **Device Management** tab:

1 Expand the tree to see the device and its policy to change.

2 Select the tunnel you want to change.

3 Right-click and select **Properties**.
The Tunnel Properties dialog box appears.

4 Make the changes you want to the tunnel.

5 Click **OK** to save the changes.
When the tunnel is renegotiated, the changes are applied.

Removing Tunnels and Devices

To remove a device from WatchGuard® System Manager (WSM), you must first remove the tunnels for which that device is an endpoint.

Removing a tunnel

1 From WSM, click the **Device Management** tab.

2 Expand the **Managed VPNs** folder to show the tunnel you want to remove.

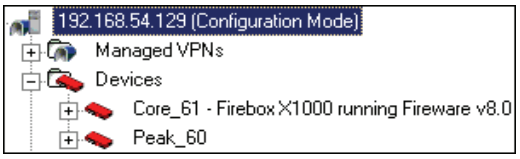
3 Right-click the tunnel.

4 Select **Remove**. Click **Yes** to confirm

5 You may have to restart the devices that use the tunnel you want to remove. Click **Yes**.

Removing a device

1 From System Manager, click the **Device Status** or **Device Management** tab.
The Device Status tab (left side figure below) or the Device Management tab (right side figure below) appears.



2 If you use the **Device Management** tab, expand the **Devices** folder to show the device to remove.

3 Right-click the device.

4 Select **Remove**. Click **Yes**.

CHAPTER 15

Configuring RUVPN with PPTP

Remote User Virtual Private Networking (RUVPN) uses Point-to-Point Tunneling Protocol (PPTP) to make a secure connection. It supports as many as 50 users at the same time for each Firebox and operates with each type of Firebox® encryption. RUVPN users can authenticate to the Firebox or to a RADIUS authentication server. You must configure the Firebox and the remote host computers of the remote user.

Configuration Checklist

Before you configure a Firebox® to use RUVPN, record this information:

- The IP addresses for the remote client to use for RUVPN sessions. **These IP addresses cannot be addresses that the network behind the Firebox uses.** The safest procedure to give addresses for RUVPN users is to install a "placeholder" secondary network with a range of IP addresses. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.0/24. Select the IP addresses in this subnet for your range of PPTP addresses. For more information, see "IP Addressing" on page 152.
- The IP addresses of the DNS and WINS servers that resolve host names to IP addresses.
- The user names and passphrases of users that are allowed to connect to the Firebox with RUVPN.

Encryption levels

Because of export limits on high encryption software, WatchGuard® Firebox products are put on the installation CD-ROM with only base encryption.

For RUVPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The Firebox always tries to use 128-bit encryption first. It uses (if enabled) 40-bit encryption if the client cannot use the 128-bit encrypted connection.

For information on how to enable the drop to 40-bit, see "Enabling RUVPN with PPTP" on page 179.

If you do not live in the U.S. and you must have strong encryption on your LiveSecurity Service account, send an e-mail to supportid@watchguard.com and include in it:

- Your LiveSecurity Service key number

- Date of purchase
- Name of your company
- Company mailing address
- Telephone number and name
- E-mail address to reply to

If you live in the U.S., you must download the strong encryption software from your archive page in the LiveSecurity Service web site. Go to www.watchguard.com, click **Support**, log in to your LiveSecurity Service account, and then click **Latest Software**. Download WatchGuard System Manager with strong encryption.

Then, uninstall WatchGuard System Manager, and install WatchGuard System Manager with strong encryption software from the downloaded file.

Note

To keep your current Firebox configuration, do not use the Quick Setup Wizard when you install the new software. Open System Manager, connect to the Firebox, and save your configuration file. Configurations with a different encryption version are compatible.

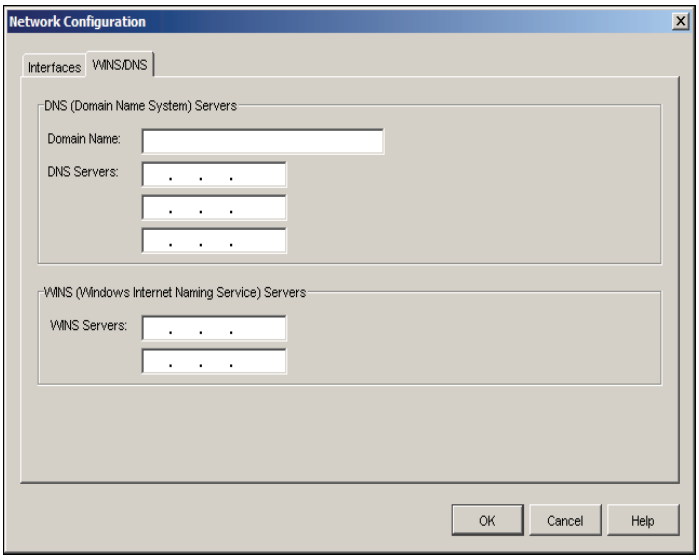
Configuring WINS and DNS Servers

RUVPN clients use shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS changes host names into IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the Firebox® must have access to these servers.

Make sure that you use an internal DNS server. Do not use external DNS servers. You must have a public DNS server if you want to use PPTP as a default gateway setting.

1 From Policy Manager, click **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.

2 In the IP address text boxes, type the addresses for the WINS and DNS servers. You can type three addresses for DNS servers, and two addresses for WINS servers. Type a domain name for the DNS server.



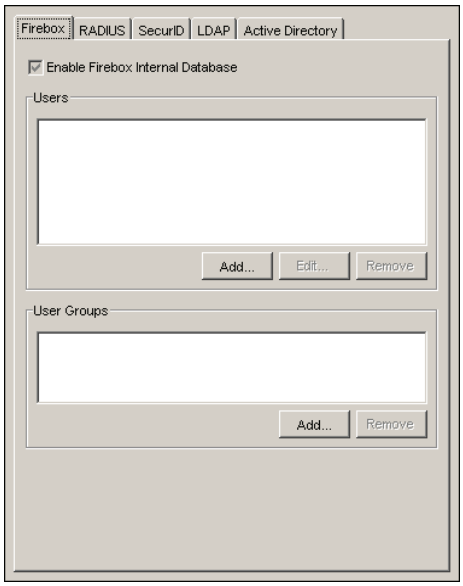
Adding New Users to Authentication Groups

To get access to Internet services (such as outgoing HTTP or outgoing FTP), the remote user gives a user name and password to authenticate. WatchGuard® System Manager software uses this information to authenticate the user to the Firebox®.

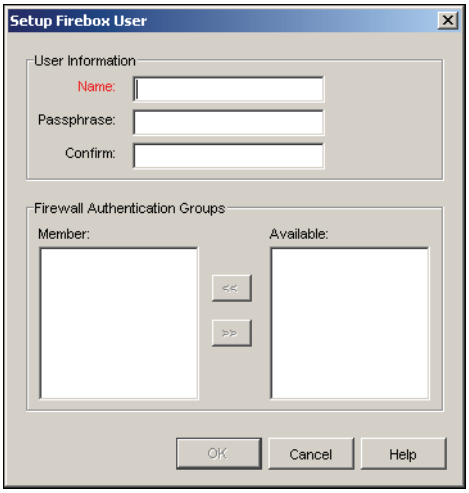
For more information on Firebox groups, see "Implementing Authentication," on page 111.

1 From Policy Manager, click **Setup > Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **Firebox** tab.



3 To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox User dialog box appears.



4 Type a user name and passphrase for the new user. Type the passphrase again to confirm it.
The new user is put on the Users list. The Authentication Servers dialog box stays open and you can add more users.

5 To close the **Authentication Servers** dialog box, click **OK**.
You can use the users and groups to configure policies. Refer to the subsequent section.

Configuring Services to Allow Incoming RUVPN Traffic

RUVPN users have no access privileges through a Firebox®. You must add user names or the full PPTP-Users group to policies. This gives remote users access to computers behind the Firebox.

WatchGuard® recommends two procedures to configure the policies for RUVPN traffic: individual policies, or the Any policy. It is best to configure individual policies to control RUVPN traffic. The Any policy opens a hole through the Firebox. This lets all the traffic flow between hosts and does not apply firewall rules. This is a security risk.

By individual policy

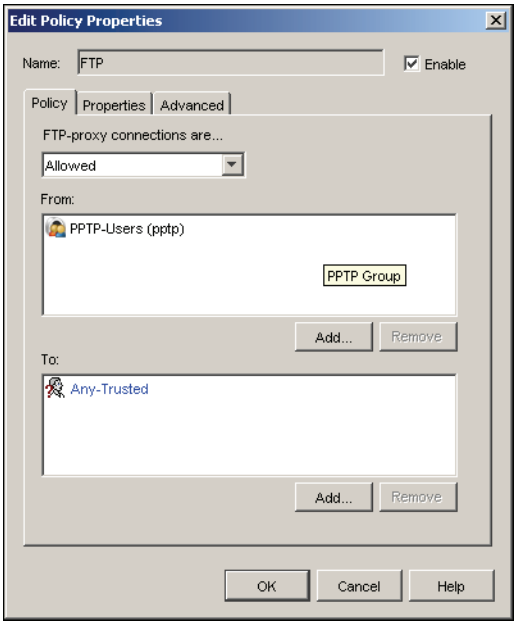
In Policy Manager, double-click a policy to enable for your VPN users. It is a good idea to create a new policy specially for PPTP traffic and keep it separate from your other firewall policies. To set the properties:

For an incoming policy:

- Allowed
- From: PPTP users or groups
- To: trusted, optional, network or host IP address, or alias

For an outgoing policy:

- Allowed
- From: trusted, optional, network or host IP address, or alias
- To: PPTP users or groups



Using the Any policies

Add Any policies with these properties:

Incoming policy:

- Allowed

- From: PPTP users or groups
- To: trusted, optional, network or host IP address, or alias

Outgoing policy:

- Allowed
- From: trusted, optional, network or host IP address, or alias
- To: PPTP users or groups

Make sure that you save your configuration file to the Firebox after you make these changes.

Note

To use WebBlocker to control the access of remote users, add PPTP users or groups to a proxy policy that controls WebBlocker, such as HTTP-proxy. Use this type of policy with any packet filter or proxy policy as an alternative to the Any policy.

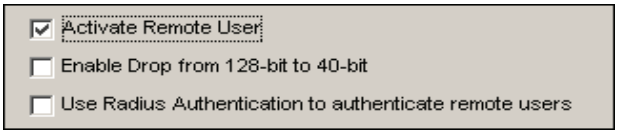
Enabling RUVPN with PPTP

To configure RUVPN with PPTP you must enable the feature. RUVPN with PPTP adds the WatchGuard® PPTP policy icon to Policy Manager. This sets default properties for PPTP connections and for the traffic that flows to and from them. We recommend that you do not change the default properties of the WatchGuard PPTP policy.

1 From Policy Manager, click **VPN > Remote Users**. Click the **PPTP** tab.

2 Select the **Activate Remote User** check box.

3 If necessary, select the **Enable Drop from 128-bit to 40-bit** check box.
Usually, only customers outside the United States use this check box.



Enabling extended authentication

RUVPN with extended authentication lets users authenticate to a RADIUS authentication server as an alternative to the Firebox®. For more information on extended authentication, see “Extended authentication” on page 151.

1 Select the **Use RADIUS Authentication to authenticate remote users** check box. Refer to the figure in the previous section.

2 Configure the RADIUS server in the **Authentication Servers** dialog box. Refer to “Implementing Authentication,” on page 111.

3 On the RADIUS server, create a PPTP-Users group and add names or groups of PPTP users.

Adding IP Addresses for RUVPN Sessions

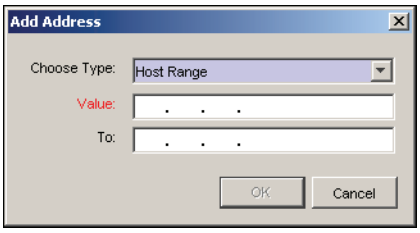
RUVPN with PPTP gives support to 50 users at the same time. The Firebox® gives an open IP address to each incoming RUVPN user from a group of available addresses. This goes on until all the addresses are

in use. After a user closes a session, the address is put back in the available group. The subsequent user who logs in gets this address.

For more information about how to get IP addresses for RUVPN clients, see “IP Addressing” on page 152. You must configure two or more IP addresses for PPTP to operate correctly.

From the **PPTP** tab on the **Remote Users Configuration** dialog box:

1 Click **Add**.
The Add Address dialog box appears.



2 From the **Choose Type** drop-down list, select **Host IP** (for a single IP address) or **Host Range** (for a range of IP addresses.
You can configure 50 addresses. If you select Host IP, you must add at least two IP addresses. If you select Host Range and add a range of IP addresses that is larger than 50 addresses, RUVPN with PPTP uses the first 50 addresses in the range.

3 In the **Value** text box, type the host IP address. If you selected **Host Range**, type the first and last IP address in the range. Click **OK**.
Type IP addresses that are not in use that the Firebox can give to clients during RUVPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.

4 Do the procedure again to configure all the addresses for use with RUVPN with PPTP.

Preparing the Client Computers

You must first prepare each computer that you use as an RUVPN with PPTP remote host, with:

- Internet service provider (ISP) account
- Public IP address.

Then, do these procedures using the instructions in the subsequent sections:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not necessary for all operating systems).

Installing MSDUN and Service Packs

It can be necessary to install these options for correct configuration of RUVPN:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- other extensions
- service packs.

For RUVPN with PPTP, it is necessary to install these upgrades::

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2

*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98, with strong encryption, Windows 2000 will automatically set strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center Web site at:

http://www.microsoft.com/downloads/search.asp

Creating and Connecting a PPTP RUVPN on Windows XP

To prepare a Windows XP remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1. Click **Start > Control Panel > Network Connections**.
   The Network Connection wizard appears.
2. Click **Create a new connection** from the menu on the left. The New Connection Wizard starts. Click **Next**.
3. Click **Connect to the network at my workplace**. Click **Next**.
4. Click **Virtual Private Network Connection**. Click **Next**.
5. Give the new connection a name, such as "Connect with RUVPN." Click **Next**.
6. Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.
   The wizard includes this screen if you use Windows XP SP2. Not all Windows XP users see this screen.
7. Type the host name or IP address of the Firebox® external interface. Click **Next**.
8. Select who can use this connection profile. Click **Next**.
9. Select **Add a shortcut to this connection to my desktop**. Click **Finish**.
10. To connect with your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.
11. Double-click the shortcut to the new connection on your desktop.
    Or, select Control Panel > Network Connections and look in the Virtual Private Network list for the connection you created.
12. Type the user name and passphrase for the connection.
    This information was given when you added the user to pptp_users. See "Adding New Users to Authentication Groups" on page 177.
13. Click **Connect**.

Creating and Connecting a PPTP RUVPN on Windows 2000

To prepare a Windows 2000 remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1 Click **Start > Settings > Network Connections > Create a New Connection**.
The New Connection wizard appears.

2 Click **Next**.

3 Select **Connect to the network at my workplace**. Click **Next**.

4 Click **Virtual Private Network connection**.

5 Give the new connection a name, such as "Connect with RUVPN." Click **Next**.

6 Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.

7 Type the host name or IP address of the Firebox® external interface. Click **Next**.

8 Select **Add a shortcut to this connection to my desktop**. Click **Finish**.

9 To connect with your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.

10 Double-click the shortcut to the new connection on your desktop.
Or, select Control Panel > Network Connections and look in the Virtual Private Network list for the connection you created.

11 Type the user name and passphrase for the connection.
This information was given when you added the user to pptp_users. See "Adding New Users to Authentication Groups" on page 177.

12 Click **Connect**.

Running RUVPN and accessing the Internet

You can enable remote users to get access to the Internet through a RUVPN tunnel. But this option has an effect on security. See "Tunneling Methods" on page 155.

1 When you set up your connection on the client computer, use the **Advanced TCP/IP Settings** dialog box to select the **Use default gateway on remote network** check box.
To open the Advanced TCP/IP Settings dialog box on Windows XP or Windows 2000, right-click the VPN connection in Control Panel > Network Connections. Select Properties and click on the Network tab. Find Internet Protocol in the list box and click Properties. On the General tab, click Advanced.

2 Make sure that the IP addresses you have added to the PPTP address pool are included in your dynamic NAT configuration. To make sure, from Policy Manager select **Network > Firewall NAT**.

3 Edit your policy configuration to allow connections from PPTP-Users through the external interface. If you use WebBlocker to control remote user Web access, add PPTP-Users to the policy that controls WebBlocker (like HTTP-proxy).

Making outbound PPTP connections from behind a Firebox

If necessary, you can make a PPTP connection to a Firebox from behind a different Firebox. For example, a remote user goes to a customer office that has a Firebox. The user can make PPTP connections to their network with PPTP. For the local Firebox to correctly allow the outgoing PPTP connection, add the PPTP policy and allow PPTP to Any-External. (For information on enabling policies, see the "Configuring Policies" chapter of this guide.)

CHAPTER 16

Advanced Networking

With Fireware™ Pro appliance software, you get access to an advanced set of networking features. These features are designed to give the Firebox® administrator more control and greater efficiency with a very large or high-traffic network. Advanced networking features include:

Multiple WAN support

You can use Fireware to configure up to four Firebox interfaces as external, or wide area network (WAN), interfaces. You can control the flow of traffic through multiple WAN interfaces to share the load of outgoing traffic.

Quality of Service (QoS)

Fireware's QoS feature lets you set priority queues, bandwidth restrictions, and connection rate limits on individual policies.

Dynamic routing

In addition to static routing, the Firebox can use the dynamic routing protocols RIP versions 1 and 2, OSPF version 2, and BGP version 4. These routing protocols allow for the dynamic modifying of routing tables.

About Multiple WAN Support

Fireware™ Pro appliance software gives you the option to configure multiple external interfaces (up to four), each on a different subnet. This allows you to connect the Firebox® to more than one Internet Service Provider (ISP). When you configure multiple external interfaces, you have two options to control which interface outgoing packets use. The options are:

Multi-WAN in round robin order

If you select "round robin" order, you can share the load of outgoing traffic among external interfaces like this:

- The first host, with IP address x.x.x.x, sends an HTTP request to the Internet. The packets in this session are sent through the lowest number external interface.
- The second host, with IP address y.y.y.y, sends an HTTP request to the Internet. The packets in this session are sent through the external interface with the second higher number.

- The third host, with IP address z.z.z.z, sends an HTTP request to the Internet. The packets in this session are sent through the lowest number external interface (if there are only two external interfaces configured) or the third higher number external interface.
- As each host initiates a connection, the Firebox cycles through external interfaces using the pattern explained above.

Multi-WAN in backup order

This option is also used only on outgoing traffic. If you select this option, the lowest number external interface configured in your list becomes the primary external interface. All other external interfaces are backup external interfaces. The Firebox sends all outgoing traffic to the primary external interface. If the primary external interface is not active, the Firebox sends traffic to the first backup interface.

The Firebox monitors the status of the primary external interface with two procedures. It checks the physical link status of the interface. It also pings the default gateway of the interface. When the Firebox detects that the primary external interface is active again, it automatically starts to send new connections to the primary external interface.

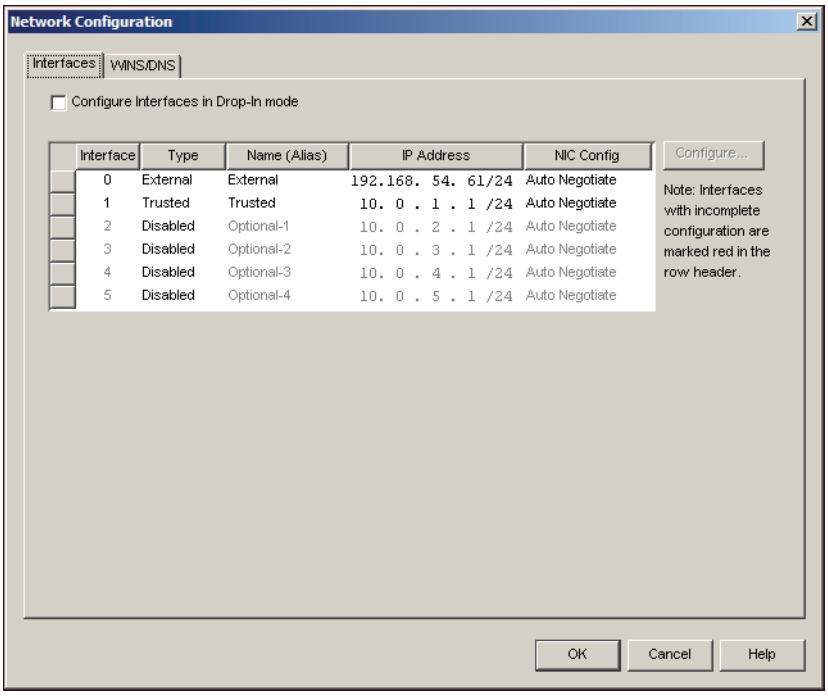
As soon as you configure a second external interface, multiple WAN support is automatically enabled with Multi-WAN in round robin order set as the default.

Note that:

- If you have a policy configured with an individual external interface alias in its configuration, you must change the configuration to use the alias "Any-External".
- You cannot use 1-to-1 NAT in a multiple WAN configuration.
- Multiple WAN support does not apply to branch office or Mobile User VPN traffic. Branch office and Mobile User VPN traffic always uses the first external interface configured for the Firebox. PPTP user VPN operates correctly in a multiple WAN configuration.
- The Multiple WAN feature is not supported in drop-in mode.

Configuring multiple WAN support

1 From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.

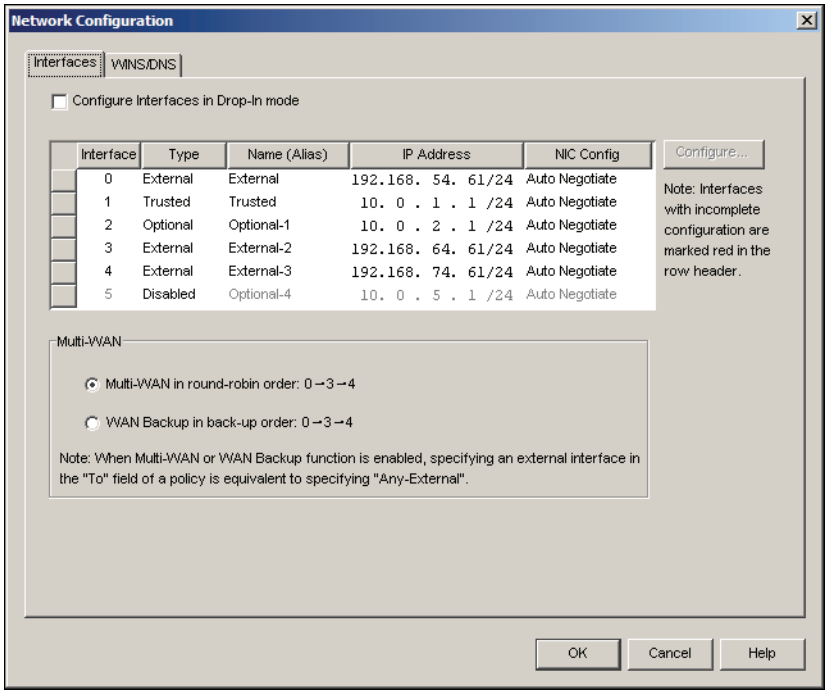

Network Configuration
Interfaces
WINS/DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
0 External External 192.168. 54. 61/24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Disabled Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 Disabled Optional-2 10. 0 . 3 . 1 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
Configure...
Note: Interfaces with incomplete configuration are marked red in the row header.
OK
Cancel
Help

2 Select the interface to configure as external and click **Configure**. Select **External** from the **Interface Type** drop-down list to activate the dialog box. Type an interface name and description.
You must have a minimum of two external network interfaces configured before you can see and configure multi-WAN settings.

3 Type the IP address and default gateway for the interface. Click **OK**.

When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

After you configure a second external interface, multiple WAN configuration options appear in the Network Configuration dialog box.


Network Configuration
Interfaces
WINS/DNS
Configure Interfaces in Drop-In mode
Interface
Type
Name (Alias)
IP Address
NIC Config
0 External External 192.168. 54. 61/24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional Optional-1 10. 0 . 2 . 1 /24 Auto Negotiate
3 External External-2 192.168. 64. 61/24 Auto Negotiate
4 External External-3 192.168. 74. 61/24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
Configure...
Note: Interfaces with incomplete configuration are marked red in the row header.
Multi-WAN
Multi-WAN in round-robin order: 0→3→4
WAN Backup in back-up order: 0→3→4
Note: When Multi-WAN or WAN Backup function is enabled, specifying an external interface in the "To" field of a policy is equivalent to specifying "Any-External".
OK
Cancel
Help

4 Select the method to use to control the flow of outgoing traffic through your multiple external interfaces. Use **Multi-WAN in round robin order** to send traffic sessions through the external interfaces in sequence. Use **Multi-WAN in backup order** to set your first external interface as primary and subsequent external interfaces as backup interfaces.

5 Click **OK**. Save your changes to the Firebox.

Creating QoS Actions

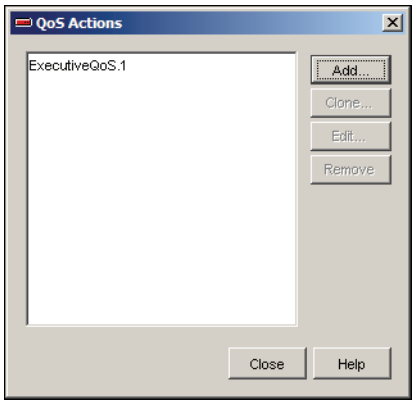
In a large network with many host computers, the volume of data that moves through the firewall can be very large. When the traffic is too much for the network, data packets are dropped. It can be necessary for a business to make traffic such as data exchanges between corporate and branch offices a higher priority than low-priority actions such as Web surfing/browsing.

With Fireware™ Pro, you can set Quality of Service (QoS) actions and apply them to policies to make sure that bandwidth for important traffic is always available.

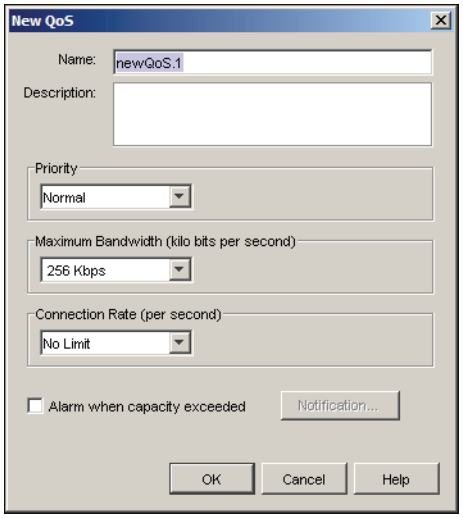
You can also define an alarm to occur when network capacity is exceeded according to the QoS action's parameters. You can configure the alarm to make the Firebox® send an event notification to the SNMP

management system, or to send a notification in the form of e-mail or a pop-up window on the management station.

1 From Policy Manager, select **Setup > Actions > QoS**.
The QoS Actions dialog box appears.



2 Click **Add**.
The New QoS dialog box appears.



3 Type the name and description of the QoS action.

4 Set **Priority** to normal or high to give traffic priority treatment.
These categories are often known as queues.

5 Use the **Maximum Bandwidth** drop-down list to change or remove the bandwidth limits for this action.
Use No Limits to remove bandwidth restrictions for important traffic, or select a maximum kilobytes per second bandwidth to allocate a part of the total available bandwidth for less important traffic.

6 Use the **Connection Rate** drop-down list to control the number of connections per second for this QoS action.
The default configuration puts no limits on the connection rate. If you select Custom, you can type the maximum connection rate for this QoS action to control the rate of bandwidth use for any traffic.

7 If you want to set an alarm when the bandwidth or connection rate is exceeded, select the **Alarm when capacity exceeded** check box. Use this alarm to determine whether a policy has a need for more bandwidth. Click **Notification** and set the notification parameters, as described in "Setting logging and notification parameters" on page 129.

8 Click **OK**.
The new action appears in the QoS Actions dialog box.

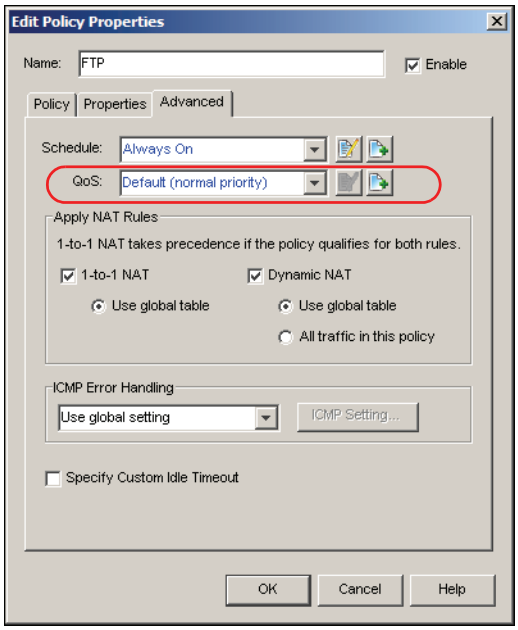
Applying QoS actions to policies

After you have created QoS actions, you can apply them to the policies you have configured in Policy Manager. To apply a QoS action:

1 From Policy Manager, double-click on the policy to which you want to add a QoS action.

2 Select the **Advanced** tab.

3 From the **QoS** drop-down list, select the QoS action to apply to the policy.



4 Use the **View/Edit** or **New/Clone** buttons (at the right of the **Schedule** and **QoS** fields) to change the properties of the QoS action or to create a new QoS action for the policy.

5 Click **OK**. Save your changes to the Firebox.

Using QoS in a multiple WAN environment

When a QoS action is applied on a multiple WAN policy with multiple WAN set up in round robin mode, the maximum bandwidth and connection rate settings in the QoS action control the total throughput and connection rate across all interfaces. This includes all external interfaces that are configured to route traffic. This also includes external interfaces that are down.

When a QoS action is applied on a multiple WAN policy with multiple WAN set up in backup mode, the maximum bandwidth and connection rate settings in the QoS action control the throughput and connection rate across the one external interface that is currently sending packets.

Dynamic Routing

A routing protocol is the language a router speaks with other routers to share information about the status of network routing tables. With static routing, routing tables are set and do not change. If a router on the remote path fails, a packet cannot get to its destination.

Dynamic routing lets routing tables in routers change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Fireware™ Pro gives support to RIP v1 and v2, OSPF, and BGP v4 dynamic routing protocols.

Routing daemon configuration files

To use any of the dynamic routing protocols with Fireware, you must import or type a dynamic routing configuration file for the routing daemon you choose. This configuration file includes information such as a password and log file name. You can find configuration templates for each of the routing protocols in this FAQ:

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

You can find a list of supported configuration commands for each routing protocol in the sections below. The command sections below appear in the order they must go in an operating configuration file.

Notes about configuration files:

- The "!" and the "#" characters are comment characters. If the first character of the word is one of the comment characters, then the rest of the line is interpreted as a comment. If the comment character is not the first character of the word, it is interpreted as a command.
- Usually, you can use the word "no" at the beginning of the line to disable a command. For example: "no network 10.0.0.0/24 area 0.0.0.0" disables the backbone area on the specified network.

Using RIP

RIP (Routing Information Protocol) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, in turn, sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. OSPF is a better alternative for larger networks.

RIP Version 1

RIP V1 uses a UDP broadcast over port 520 to send updates to routing tables. To create or modify a routing configuration file, here is a table of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample RIP configuration file found in this FAQ:

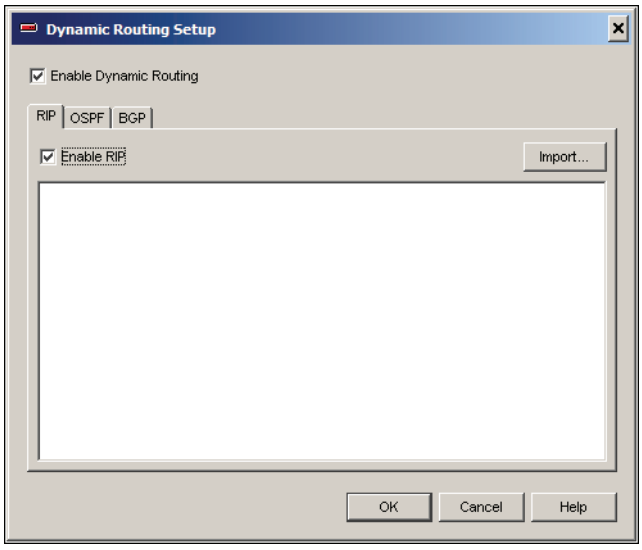
https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

Section	Command	Description
Set simple password or MD5 authentication on an interface		
	interface eth[N]	Begin section to set authentication type for interface
	ip rip authentication string [PASSWORD]	Set RIP authentication password
	key chain [KEY-CHAIN]	Set MD5 key chain name
	key [INTEGER]	Set MD5 key number
	key-string [AUTH-KEY]	Set MD5 authentication key
	interface eth[N]	Begin section to set authentication type for interface
	ip rip authentication mode md5	Use MD5 authentication
	ip rip authentication mode key-chain [KEY-CHAIN]	Set MD5 authentication key-chain
Configure RIP routing daemon		
	router rip	Enable RIP daemon
	version [1|2]	Set RIP version to 1 or 2 (default version 2)
	ip rip send version [1|2]	Set RIP to send version 1 or 2
	ip rip receive version [1|2]	Set RIP to receive version 1 or 2
	no ip split-horizon	Disable split-horizon; enabled by default
Configure interfaces and networks		
	no network eth[N]	
	passive-interface eth[N]	
	passive-interface default	
	network [A.B.C.D/M]	
	neighbor [A.B.C.D/M]	
Distribute routes to RIP peers and inject OSPF or BGP routes to RIP routing table		
	default-information originate	Share route of last resort (default route) with RIP peers
	redistribute kernel	Redistribute firewall static routes to RIP peers
	redistribute connected	Redistribute routes from all interfaces to RIP peers
	redistribute connected route-map [MAPNAME]	Redistribute routes from all interfaces to RIP peers, with a route map filter (mapname)
	redistribute ospf	Redistribute routes from OSPF to RIP
	redistribute ospf route-map [MAPNAME]	Redistribute routes from OSPF to RIP, with a route map filter (mapname)
	redistribute bgp	Redistribute routes from BGP to RIP
	redistribute bgp route-map [MAPNAME]	Redistribute routes from BGP to RIP, with a route map filter (mapname)
Configure route redistribution filters with route maps and access lists		

Section	Command	Description
	access-list [PERMIT | DENY] [LISTNAME] [A.B.C.D/M | ANY]	Create an access list to only allow or deny redistribution of an IP address or of any
	route-map [MAPNAME] permit [N]	Create a route map with a name and allow with a priority of N
	match ip address [LISTNAME]	

Configuring Fireware to use RIP v1

1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click **Enable Dynamic Routing** and **Enable RIP**.

3 Click **Import** to import a routing daemon configuration file, or type your configuration file in the text box.
If you click Import, you can browse to the location of the RIP daemon configuration template. It is located in C:\Documents and Settings\My Documents\My WatchGuard.

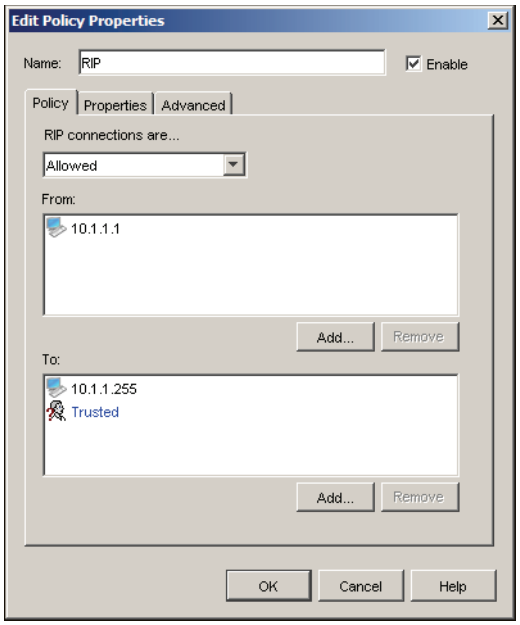
4 Click **OK**.

Allowing RIP v1 traffic through the Firebox

You must add and configure a policy to allow RIP broadcasts from the router to the network broadcast IP address. You must also add the IP address of the Firebox interface to the **To** field.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**.
The New Policy Properties window appears for RIP.

2 In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the Firebox® interface it connects to. You must also add the network broadcast IP address.



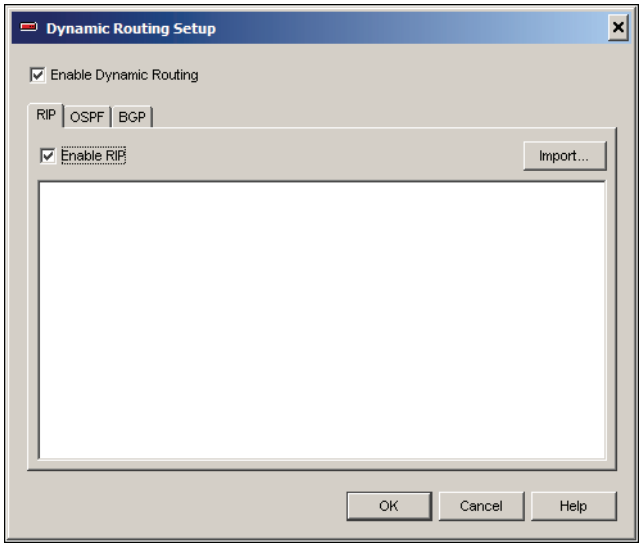
3 Click **OK**.

RIP Version 2

RIP v2 uses multicast to send routing table updates. To create or modify a routing configuration file, refer to the table of supported RIP routing commands in the section *RIP Version 1*. Any command that uses a network IP address must include the subnet mask or RIP v2 will not operate. The sections must appear in the configuration file in the same order they appear in this table.

Configuring Fireware to use RIP v2

1 In Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click **Enable Dynamic Routing** and **Enable RIP**.

3 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.
If you click Import, you can browse to the location of the RIP daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.

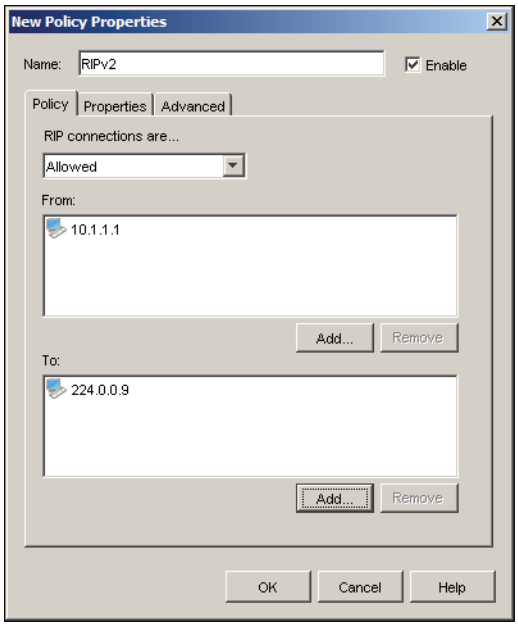
4 Click **OK**.

Allowing RIP v2 traffic through the Firebox

You must add and configure a policy to allow RIP v2 multicasts from the routers that have RIP v2 enabled to the reserved multicast IP address for RIP v2.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**.
The New Policy Properties window appears for RIP.

2 In the **New Policy Properties** window, configure the policy to allow traffic from the IP or network address of the router using RIP to the multicast address 224.0.0.9.



3 Click **OK**.

Using OSPF

OSPF (Open Shortest Path First) is an interior router protocol used in larger networks. With OSPF, a router that sees a change to its routing table or that detects a change in the network immediately sends a multicast update to all other routers in the network. OSPF is different than RIP because:

- OSPF sends only the part of the routing table that has changed in its transmission. RIP sends the full routing table each time.
- OSPF sends a multicast only when its information has changed. RIP sends the routing table each 30 seconds.

OSPF Daemon Configuration

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample OSPF configuration file found in the FAQ:

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

Section	Command	Description
Configure Interface		
	ip ospf authentication-key [PASSWORD]	Set OSPF authentication password
	interface eth[N]	Begin section to set properties for interface

Section	Command	Description
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Set MD5 authentication key ID and key
	ip ospf cost [1-65535]	Set link cost for the interface (see OSP Interface Cost table below)
	ip ospf hello-interval [1-65535]	Set interval to send hello packets; default is 10 seconds
	ip ospf dead-interval [1-65535]	Set interval after last hello from a neighbor before declaring it down; default is 40 seconds
	ip ospf retransmit-interval [1-65535]	Set interval between link-state advertisements (LSA) retransmissions; default is 5 seconds
	ip ospf transmit-delay [1-3600]	Set time required to send LSA update; default is 1 second
	ip ospf priority [0-255]	Set router priority; high value increases eligibility to become the designated router (DR)
Configure OSPF Routing Daemon		
	router ospf	Enable OSPF daemon
	ospf router-id [A.B.C.D]	Set router ID for OSPF manually; router will determine its own ID if not set
	ospf rfc 1583compatibility	Enable RFC 1583 compatibility (can lead to routing loops)
	ospf abr-type [cisco|ibm|shortcut|standard]	More information about this command can be found in draft-ietf-abr-alt-o5.txt
	passive interface eth[N]	Disable OSPF announcement on interface eth[N]
	auto-cost reference bandwidth [0-429495]	Set global cost (see OSPF cost table below); do not use with "ip ospf [COST]" command
	timers spf [0-4294967295][0-4294967295]	Set SPF schedule delay and hold time
Enable OSPF on a Network *The "Area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	network [A.B.C.D/M] area [Z]	Announce OSPF on network A.B.C.D/M for area 0.0.0.Z
Configure Properties for Backbone Area or Other Areas *The "Area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	area [Z] range [A.B.C.D/M]	Create area 0.0.0.Z and set a classful network for the area (range and interface network and mask settings should match)
	area [Z] virtual-link [W.X.Y.Z]	Set virtual link neighbor for area 0.0.0.Z
	area [Z] stub	Set area 0.0.0.Z as a stub
	area [Z] stub no-summary	
	area [Z] authentication	Enable simple password authentication for area 0.0.0.Z
	area [Z] authentication message-digest	Enable MD5 authentication for area 0.0.0.Z

Section	Command	Description
Redistribute OSPF Routes		
	default-information originate	Share route of last resort (default route) with OSPF
	default-information originate metrics [0-16777214]	Share route of last resort (default route) with OSPF
	default-information originate always	Share route of last resort (default route) with OSPF
	default-information originate always metrics [0-16777214]	Share route of last resort (default route) with OSPF
	redistribute connected	Redistribute routes from all interfaces to OSPF
	redistribute connected metrics	Redistribute routes from all interfaces to OSPF
Configure Route Redistribution with Access Lists and Route Maps		
	access-list [LISTNAME] permit [A.B.C.D/M]	Create an access list to allow distribution of A.B.C.D/M
	access-list [LISTNAME] deny any	Restrict distribution of any route map not specified above
	route-map [MAPNAME] permit [N]	Create a route map with name [MAPNAME] and allow with a priority of [N]
	match ip address [LISTNAME]	

OSPF Interface Cost table

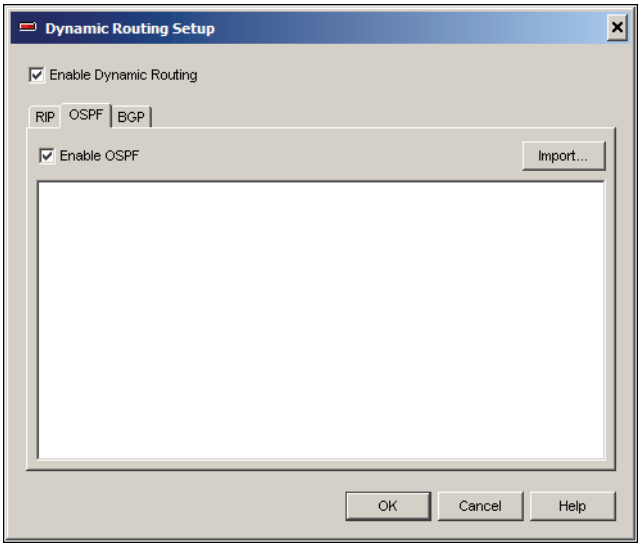
The OSPF protocol finds the most efficient route between two points. To do this, it looks at factors such as interface link speed, the number of hops between points, and other metrics. By default, OSPF uses the actual link speed of a device to calculate the total cost of a route. You can set the interface cost manually to help maximize efficiency if, for example, your gigabyte-based firewall is connected to a 100M router. Use the numbers in the OSPF Interface Cost table to manually set the interface cost to a value different than the actual interface cost.

Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Ethernet	1G	100M	1
Ethernet	100M	10M	10
Ethernet	10M	1M	100
Modem	2M	200K	500
Modem	1M	100K	1000
Modem	500K	50K	2000
Modem	250K	25K	4000
Modem	125K	12500	8000
Modem	62500	6250	16000
Serial	115200	9216	10850
Serial	57600	4608	21700
Serial	38400	3072	32550

Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Serial	19200	1636	61120
Serial	9600	768	65535

Configuring Fireware to use OSPF

1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click the **OSPF** tab.

3 Click **Enable Dynamic Routing** and **Enable OSPF**.

4 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.
If you click Import, you can browse to the location of the OSPF daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.

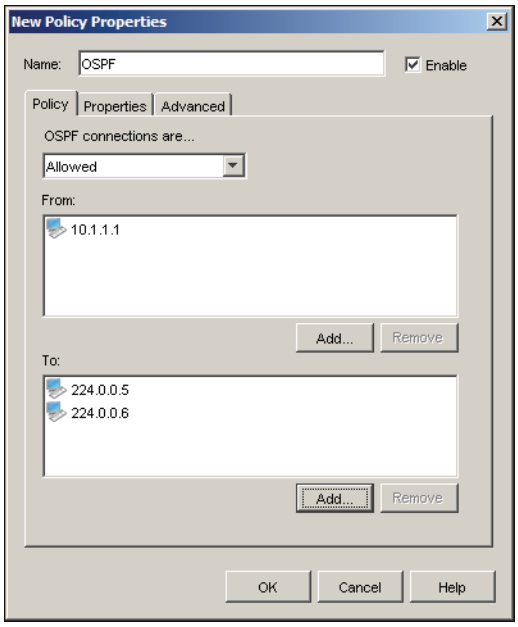
5 Click **OK**.

Allowing OSPF traffic through the Firebox

You must add and configure a policy to allow OSPF multicasts from the routers that have OSPF enabled to the reserved multicast addresses for OSPF.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **OSPF**. Click **Add**.
The New Policy Properties window appears for OSPF.

2 In the **New Policy Properties** window, configure the policy to allow traffic from the IP or network address of the router using OSPF to the IP addresses 224.0.0.5 and 224.0.0.6. Click **OK**.



Using BGP

The Border Gateway Protocol (BGP) is a scalable dynamic routing protocol used by groups of routers to share routing information. BGP is the routing protocol used on the Internet. BGP uses route parameters or "attributes" to define routing policies and create a stable routing environment.

Hosts using BGP use TCP to send updated routing table information when one host finds a change. The host sends only the part of the routing table that has the change. BGP uses classless interdomain routing (CIDR) to reduce the size of the Internet routing tables. The size of the BGP routing table in Fireware™ Pro is set at 32K.

The size of the typical WatchGuard® customer wide area network (WAN) is best suited for OSPF dynamic routing. A WAN can also use external border gateway protocol (EBGP) when more than one gateway to the Internet is available. EBGP allows you to take full advantage of the redundancy possible with a multi-homed network.

To participate in EBGP with an ISP you must have an autonomous system number (ASN). You must get an ASN from one of the regional registries in the table below. After you are assigned your own ASN you must contact each ISP to get their AS numbers and other necessary information.

Region	Registry Name	Web Site
North America	ARIN	www.arin.net
Europe	RIPE NCC	www.ripe.net
Asia Pacific	APNIC	www.apnic.net
Latin America	LACNIC	www.lacnic.net
Africa	AfriNIC	www.afrinic.net

BGP Daemon Configuration

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample BGP configuration file found in this FAQ:

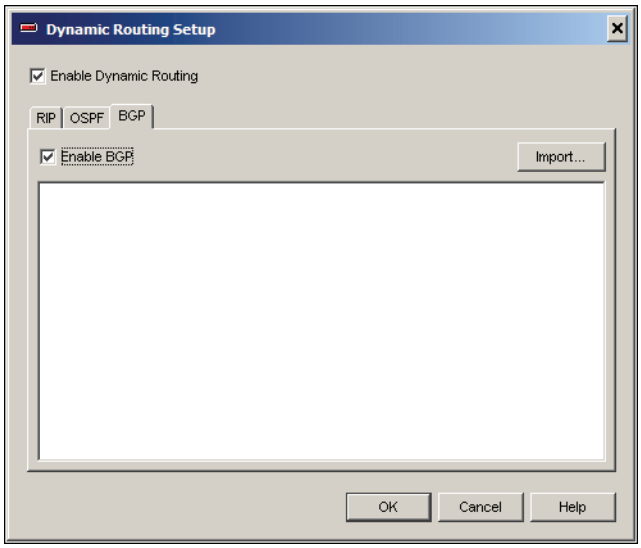
https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

Section	Command	Description
Configure BGP Routing Daemon		
	router bgp [ASN]	Enable BGP daemon and set autonomous system number (ASN); this is supplied by your ISP
	network [A.B.C.D/M]	Announce BGP on network A.B.C.D/M
	no network [A.B.C.D/M]	Disable BGP announcements on network A.B.C.D/M
Set Neighbor Properties		
	neighbor [A.B.C.D] remote-as [ASN]	Set neighbor as member of remote ASN
	neighbor [A.B.C.D] ebgp-multihop	Set neighbor on another network using EBGP multi-hop
	neighbor [A.B.C.D] version 4+	Set BGP version (4, 4+, 4-) for communication with neighbor; default is 4
	neighbor [A.B.C.D] update-source [WORD]	Set the BGP session to use a specific interface for TCP connections
	neighbor [A.B.C.D] default-originate	Announce default route to BGP neighbor [A.B.C.D]
	neighbor [A.B.C.D] port 189	Set custom TCP port to communicate with BGP neighbor [A.B.C.D]
	neighbor [A.B.C.D] send-community	Set peer send-community
	neighbor [A.B.C.D] weight 1000	Set a default weight for neighbor's [A.B.C.D] routes
	neighbor [A.B.C.D] maximum-prefix [NUMBER]	Set maximum number of prefixes allowed from this neighbor
Community Lists		
	ip community-list [<1-99>|<100-199>] permit AA:NN	Specify community to accept autonomous system number and network number separated by a colon are entered as the new community format.
Peer Filtering		
	neighbor [A.B.C.D] distribute-list [LISTNAME] [IN|OUT]	Set distribute list and direction for peer
	neighbor [A.B.C.D] prefix-list [LISTNAME] [IN|OUT]	To apply a prefix list to be matched to incoming advertisements or outgoing advertisements to that neighbor
	neighbor [A.B.C.D] filter-list [LISTNAME] [IN|OUT]	To match an autonomous system path access list to incoming routes or outgoing routes

Section	Command	Description
	neighbor [A.B.C.D] route-map [MAPNAME] [IN|OUT]	To apply a route map to incoming or outgoing routes
Redistribute Routes to BGP		
	redistribute kernel	Redistribute static routes to BGP
	redistribute rip	Redistribute RIP routes to BGP
	redistribute ospf	Redistribute OSPF routes to BGP
Route Reflection		
	bgp cluster-id A.B.C.D	To configure the cluster ID if the BGP cluster has more than one route reflector
	neighbor [W.X.Y.Z] route-reflector-client	To configure the router as a BGP route reflector and configure the specified neighbor as its client
Access Lists and IP Prefix Lists		
	ip prefix-list PRELIST permit A.B.C.D/E	Set prefix list
	access-list NAME [deny|allow] A.B.C.D/E	Set access list
	route-map [MAPNAME] permit [N]	In conjunction with the "match" and "set" commands, this defines the conditions and actions for redistributing routes
	match ip address prefix-list [LISTNAME]	Matches the specified access_list
	set community [A:B]	Set the BGP community attribute
	match community [N]	Matches the specified community_list
	set local-preference [N]	Sets the preference value for the autonomous system path

Configuring Fireware to use BGP

1 From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2 Click the **BGP** tab.

3 Click **Enable Dynamic Routing** and **Enable BGP**.

4 Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box.

If you click Import, you can browse to the location of the BGP daemon configuration file. It is located in C:\Documents and Settings\My Documents\My WatchGuard.

5 Click **Select a BGP Configuration** file. Click **OK**.

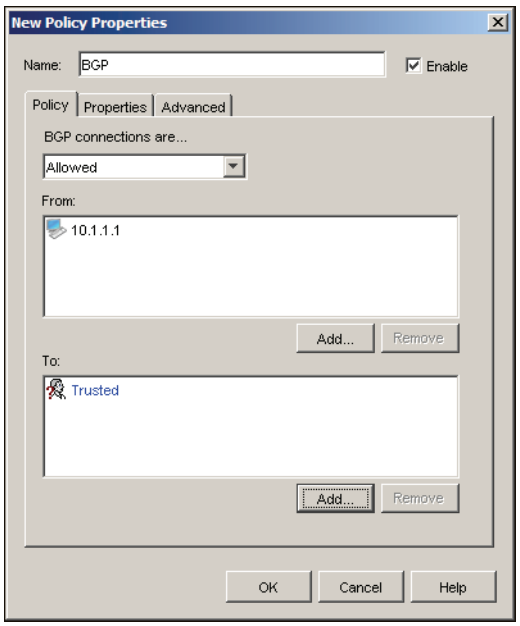
Allowing BGP traffic through the Firebox

You must add and configure a policy to allow BGP traffic to the Firebox® from the approved networks. These networks must be the same networks you defined in your BGP configuration file.

1 From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **BGP**. Click **Add**.

The New Policy Properties window appears for BGP.

2 In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router using BGP to the Firebox interface it connects to. Click **OK**.



CHAPTER 17

Controlling Web Site Access with WebBlocker

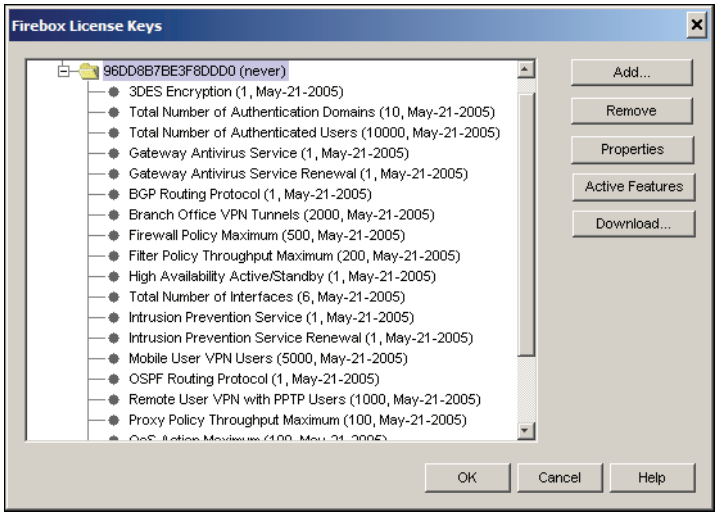
The WebBlocker feature of WatchGuard® Fireware™ Pro uses the HTTP proxy to control web traffic. You can select the exact hours in the day that users can browse the Internet. You can also select categories of web sites that users cannot go to.

Installing the Software Licenses

To install WebBlocker, you must have a WebBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

To install this feature key:

1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.


Firebox License Keys
96DD8B7BE3F8DDD0 (never)
3DES Encryption (1, May-21-2005)
Total Number of Authentication Domains (10, May-21-2005)
Total Number of Authenticated Users (10000, May-21-2005)
Gateway Antivirus Service (1, May-21-2005)
Gateway Antivirus Service Renewal (1, May-21-2005)
BGP Routing Protocol (1, May-21-2005)
Branch Office VPN Tunnels (2000, May-21-2005)
Firewall Policy Maximum (500, May-21-2005)
Filter Policy Throughput Maximum (200, May-21-2005)
High Availability Active/Standby (1, May-21-2005)
Total Number of Interfaces (6, May-21-2005)
Intrusion Prevention Service (1, May-21-2005)
Intrusion Prevention Service Renewal (1, May-21-2005)
Mobile User VPN Users (5000, May-21-2005)
OSPF Routing Protocol (1, May-21-2005)
Remote User VPN with PPTP Users (1000, May-21-2005)
Proxy Policy Throughput Maximum (100, May-21-2005)
Add...
Remove
Properties
Active Features
Download...
OK
Cancel
Help

2 Click **Remove** to remove the current feature key.

3 Click **Add**.

4 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

Getting Started with WebBlocker

You can install the WebBlocker server on your WatchGuard® management station when you first do the setup for WatchGuard System Manager. You can also install the WebBlocker Server software on a different computer using the same method as you used to install the System Manager software, but you select only the WebBlocker Server component.

Operating systems that are supported for the WebBlocker server are Windows NT 4.0, Windows 2000, and Windows 2003.

Note

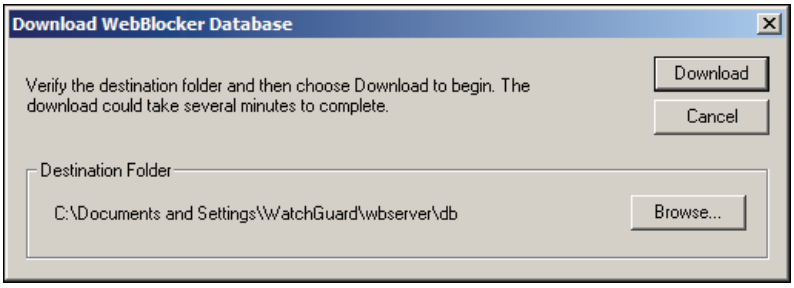
If you install one of the WSM servers on a computer with a personal firewall other than the Microsoft Windows firewall, you must open the ports for the servers to connect through the firewall. To allow connections to the WebBlocker Server, open UDP port 5003. It is not necessary to change your configuration if you use the Microsoft Windows firewall. See the *WatchGuard System Manager User Guide* for more information.

Before you configure WebBlocker, you must download the WebBlocker database.

1 Right-click the WebBlocker Server icon in the toolbar at the bottom of the screen.

2 Select **Get Full Database**.
The Download WebBlocker Database dialog box appears.

3 Select **Download** to download the new database.


Download WebBlocker Database
Verify the destination folder and then choose Download to begin. The download could take several minutes to complete.
Download
Cancel
Destination Folder
C:\Documents and Settings\WatchGuard\wbserver\db
Browse...

Note

The WebBlocker database has more than 95 MB of data. Your connection speed sets the download speed, and the download can be more than 30 minutes. Make sure the hard disk drive has a minimum of 200 MB of free space.

You can use the WebBlocker utility at any time to:

- Download a new version of the database.
- Get an incremental update of the database.
- See the database status.
- Start or stop the server.

Automating WebBlocker database downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. Before you can do this, you must download the WebBlocker database and start the WebBlocker Server. Then, you can use Windows Task Scheduler to schedule the "updatedb.bat" process, which is created automatically for you in your WSM8/bin directory when the WebBlocker Server is started.

1 Open **Scheduled Tasks**. To open the Task Scheduler using Windows XP, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.

2 Click **Add Scheduled Task**.

3 The Scheduled Tasks wizard starts. Click **Next**.

4 The screen shows a list of programs. Click **Browse**.

5 Go to C:\Program Files\WatchGuard\wsm8\bin. Select `updatedb.bat`.

6 Select the time interval at which to do this task. We recommend that you update your database each day. You can update less frequently if you have low bandwidth. Click **Next**.

7 Type the time and frequency to start the procedure. Because you must stop the WebBlocker Server to do the update, we recommend that you schedule updates outside of your usual hours of operation.

8 Select a start date. Click **Next**.

9 Type the user name and the password to use this procedure. Make sure that this user has access to the necessary files. Click **Next**.

10 Click **Finish**.

Activating WebBlocker

Before you use WebBlocker in an HTTP proxy policy, you must use the Activate WebBlocker wizard to activate the feature and create a basic configuration. To do this:

1 From WatchGuard® System Manager, select the Firebox that will use WebBlocker.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manger toolbar.

3 From Policy Manager, select **Tasks** > **WebBlocker** > **Activate**.
The Activate WebBlocker wizard starts.

4 Click **Next**.

5 Click through the wizard and add the information it asks for. The wizard has the following screens:

Select policies for WebBlocker

This screen does not appear if you have not yet defined any HTTP proxy policies. In this case, the wizard will create an HTTP proxy policy for you.

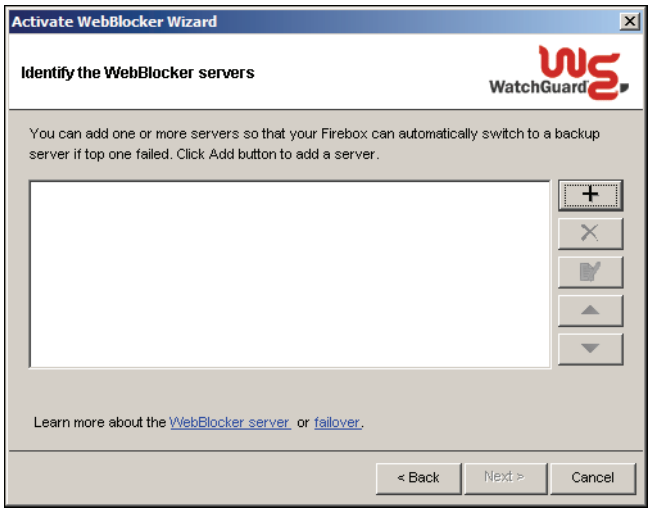
If HTTP proxy policies are already created on your Firebox, this screen shows them in a list. From the list, select the proxy policies you want to enable WebBlocker for. If no policy is selected, a new HTTP proxy policy is created with a WebBlocker action.

Identify the WebBlocker Servers

You must configure a minimum of one WebBlocker Server. To add a WebBlocker Server, click the plus sign (+). Next to **Server IP**, type the IP address of the WebBlocker Server. If necessary, change the port number.

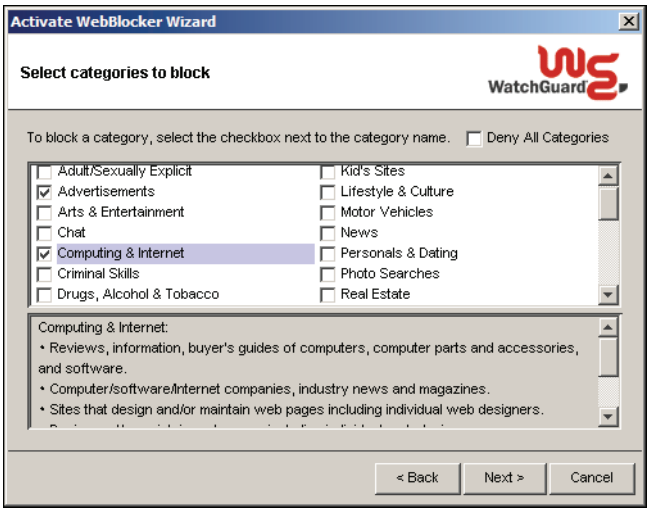
You can add more than one WebBlocker Server so the Firebox can fail over to a backup server if it cannot connect to the primary server. The first server in the list is the primary server.

To add a WebBlocker Server after you complete the wizard, go to **Setup > Actions > WebBlocker**. Add servers on the **Servers** tab.


Activate WebBlocker Wizard
Identify the WebBlocker servers
WatchGuard
You can add one or more servers so that your Firebox can automatically switch to a backup server if top one failed. Click Add button to add a server.
Learn more about the WebBlocker server or failover.
< Back
Next >
Cancel

Select categories to block

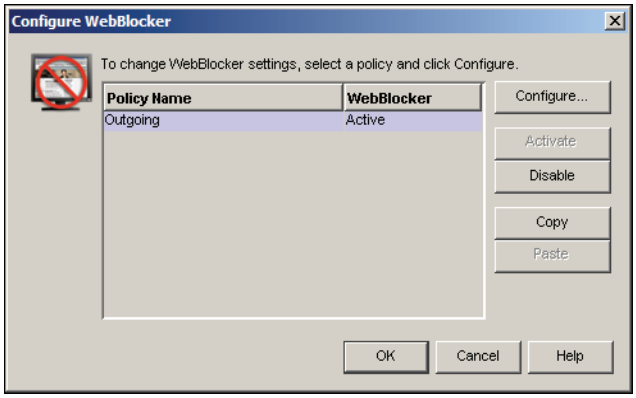
Select the check box adjacent to the categories of web sites you want to block. To read a description of the category, select the check box adjacent to it. The description appears in the box at the bottom of the screen. If you want to block access to web sites that match any category, select **Deny All Categories**.



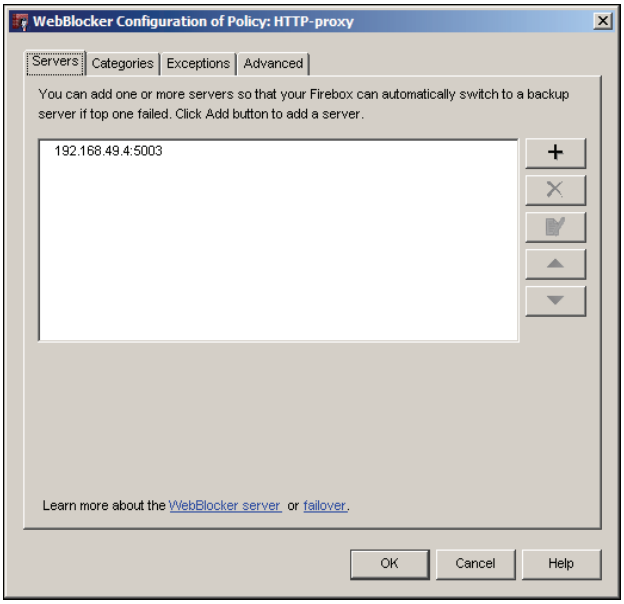
Configuring WebBlocker

After you use the Activate WebBlocker wizard to activate WebBlocker and create a basic configuration, you can configure more WebBlocker settings.

1 From Policy Manager, select **Tasks** > **WebBlocker** > **Configure**.
The Configure WebBlocker dialog box appears and shows the HTTP policies that were already created.



2 Select the policy you want to configure and click **Configure**.
The WebBlocker Configuration dialog box for that policy appears.


WebBlocker Configuration of Policy: HTTP-proxy
Servers
Categories
Exceptions
Advanced
You can add one or more servers so that your Firebox can automatically switch to a backup server if top one failed. Click Add button to add a server.
192.168.49.4:5003
Learn more about the WebBlocker server, or failover.
OK
Cancel
Help

The **WebBlocker Configuration** dialog box includes tabs to configure servers, categories, exceptions, and advanced settings.

Adding new servers

You can add more than one WebBlocker Server so the Firebox can fail over to a backup server if it cannot connect to the primary server. The first server in the list is the primary server. You can not add more than five WebBlocker Servers to a configuration.

1 To add a server, click the plus sign (+).
The Add WebBlocker Server dialog box appears.
2 Next to **Server IP**, type the IP address of the WebBlocker Server. Type the port number.

Selecting categories to block

When you used the Activate WebBlocker wizard, you selected categories of web sites you want to block. You can use this dialog box to make changes to your original configuration. Select the check box adjacent to the categories of web sites you want to block. To read a description of the category, click on it. The description appears in the box at the bottom of the screen. If you want to block access to web sites that match any category, select **Deny All Categories**.

Defining WebBlocker exceptions

You can override a WebBlocker action with an exception. You can add a web site that is allowed or denied as an exception to the WebBlocker categories. The web sites you add apply only to HTTP traffic. They are not related to the Blocked Sites list.

The exceptions are based on URL patterns, not IP addresses. You can select to have the Firebox block an URL with an exact match. Usually, it is more convenient to have the Firebox look for URL patterns. The URL patterns do not include the leading "http://". To match a URL path on all web sites, the pattern must have a leading "/*".

The host in the URL can be the host name specified in the HTTP request, or the IP address of the server.

Network addresses are not supported at this time, though you can use subnets in a pattern (for example, 10.0.0.*).

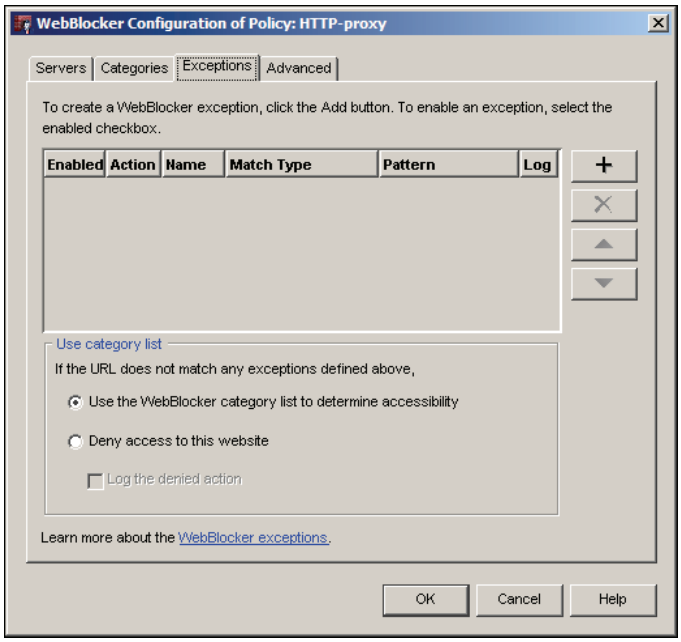
For servers on port 80, do not include the port. For servers on ports other than 80, add " :port", for example: 10.0.0.1:8080. You can also use a wildcard for the port—for example,10.0.0.1:*—but this does not apply to port 80.

You can also create exceptions with the use of any part of a URL. You can set a port number, path name, or string that must be blocked for a special web site. For example, if it is necessary to block only www.sharedspace.com/~dave because it has inappropriate photographs, you type "www.sharedspace.com/~dave/*". This gives the users the ability to browse to www.sharedspace.com/~julia, which contains content on increased production.

To block URLs that contain the word "sex" in the path, you can type "*/*sex*". To block URLs that contain "sex" in the path or the host name, type "*sex*".

You can block ports in an URL. For example, look at the URL http://www.hackerz.com/warez/index.html:8080. This URL has the browser use the HTTP protocol on TCP port 8080 instead of the default method that uses TCP 80. You can block the port by matching *8080.

1 To define exceptions to the WebBlocker categories, click the **Exceptions** tab.



2 Click the "+" sign to add a new exception rule.

3 Click the **Action** column to get access to the **Action** drop-down list. Select to have WebBlocker allow or deny the exception.

4 Type a name for the exception in the **Name** text box.

5 Click the **Match Type** column to get access to the **Match Type** drop-down list:

Pattern match: Be sure to drop the leading "http://" and include "/* at the end.

Exact match: Select this to match character by character. If you enter an exception to allow www.yahoo.com as an exact match only, and a user types "www.yahoo.com/news", the request is denied.

Regular expression: Supports wild cards used in shell script

6 Type the pattern you want to identify as an exception in the **Pattern** text box.

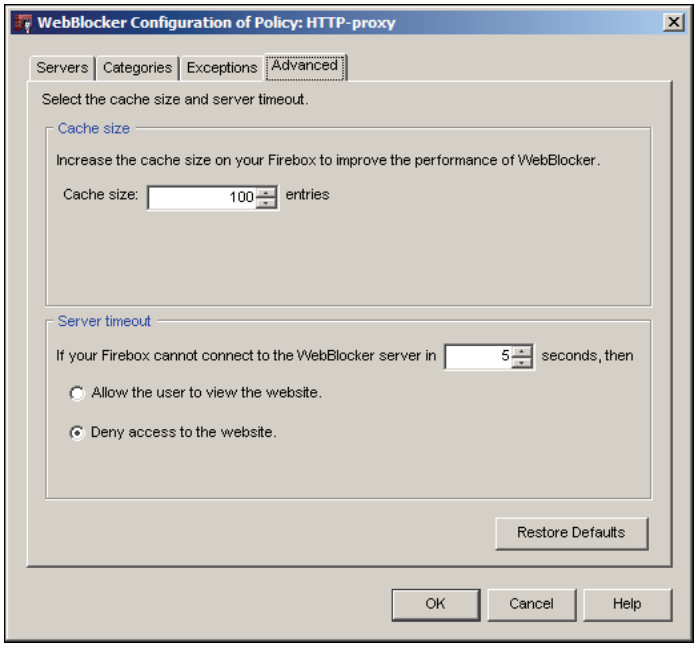
7 Click the **Log** check box if you want a log message when an action is taken on a WebBlocker exception.

8 To enable the exception, click the **Enabled** check box.

9 In the **Use category list** section, you can configure the action to occur if the URL does not match the exceptions you configure. If you want to use the list on the **Categories** tab to determine accessibility, click the top radio button. If you want to deny access, click the bottom radio button. If you deny access, you can select the check box below the radio button to send a log message for that action.

Defining advanced WebBlocker options

1 To configure advanced WebBlocker options, click the **Advanced** tab.



2 You can adjust the **Cache size** setting to improve WebBlocker performance. Use the arrows to change the number of entries in the cache or type in a number.

3 You can set a time-out value and an action to occur when the server times out. If you want to allow the web site if the server times out, select **Allow the user to view the website**. If you want to deny the web site, select **Deny access to the website**.

Scheduling a WebBlocker Action

You can set an operating schedule for the policy. You can use the predefined settings in the drop-down list or create custom schedules. You use these time periods to set rules for when to block different web sites. For example, you can block sports web sites during usual business hours of operation, but allow users to browse at lunch time, evenings, and weekends.

To set a schedule for a policy

1 Open the policy to edit it, and click the **Advanced** tab.

2 Select a schedule from the drop-down list, or click the New/Clone icon to make a new schedule. For more information, see “Creating Schedules” on page 50.

3 Configure an HTTP policy that uses the schedule.

You can also configure two HTTP policies, but create a schedule for only one of them. Each policy uses one of the HTTP proxy actions. Each of these HTTP proxy actions points to one of at least two Web-Blocker actions.

CHAPTER 18

High Availability

High Availability (HA) refers to the ability of a network to operate when a hardware or software fails. When you add redundancy to your network, you remove one point of vulnerability.

The WatchGuard® High Availability feature enables the installation of two Firebox® devices in a failover configuration. The configuration includes one Firebox we identify as the primary device and the other we identify as the secondary device. One of these devices is always in active mode and the other in standby mode. These two Fireboxes are known as "peers." They constantly send messages to each other to communicate their status.

When a failover event occurs, the standby system becomes active. After a Firebox becomes active, it stays active until it goes offline and the standby Firebox starts as the active unit.

High Availability Requirements

Here are the requirements for the High Availability feature:

- You must have one High Availability license for each HA pair. We recommend that you use the Firebox® with the maximum license features and capacities as the primary HA device.
- The two Fireboxes in an HA configuration must be the same model and must use the same software version. If the software versions are different, you must upgrade the Firebox with the old version to match the other Firebox. The Firebox with the old software must have a license for the upgraded software.
- The two Fireboxes must connect to your network in the same method. For example, the external interfaces of each must connect to the same hub or switch.
- For a Firebox X Core, you can configure the High Availability connection on the eth5 port or on eth5 and eth4. For a Firebox X Peak, use the eth9 port or eth8 and eth9. We recommend that you connect the ports after you configure them.
- HA does not operate correctly if one of the Fireboxes in the HA pair is a VPN endpoint in a VPN tunnel created and managed by the Management Server.

Note

High availability requires an interface or interfaces dedicated specifically for HA. The HA interface supports only host-to-host traffic and not network traffic.

Installing High Availability

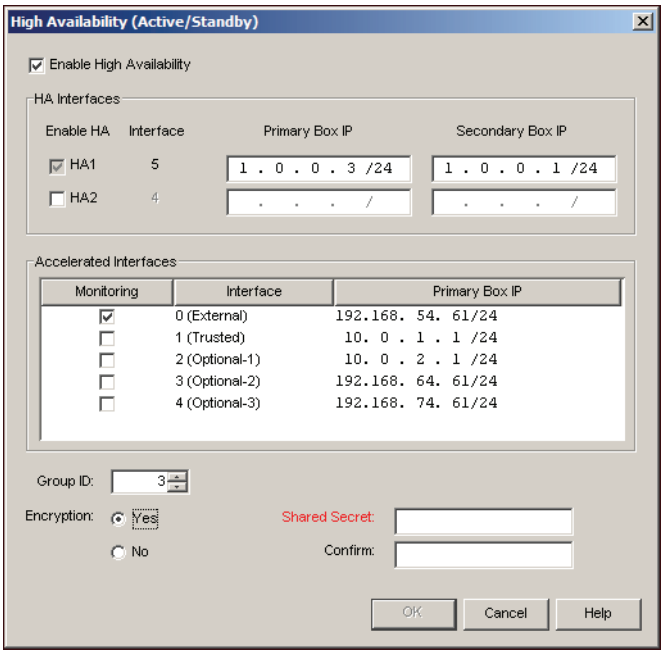
When you purchase the High Availability upgrade, you receive a certificate. Use the instructions on the certificate to go to the LiveSecurity® Service web site and activate your upgrade. After you activate the upgrade, you get a High Availability license key. You must add a unique High Availability license key to the primary Firebox in the High Availability pair. Each Firebox® in the pair must have the same version of WatchGuard System Manager software and firmware.

You must add the High Availability license to the configuration file of the primary Firebox. (We recommend you use the Firebox with the most features as the primary Firebox.) Both Fireboxes in the High Availability pair will use the license features of the primary Firebox. If you purchase upgrades for your High Availability pair, you must apply the upgrade to the serial number of the primary Firebox when you activate the upgrade on the LiveSecurity Web site.

If you use IPSec VPN tunnels that use a VPN certificate for authentication, the secondary Firebox must get its own IPSec VPN certificate. Only the Management Server certificate is copied from the primary Firebox to the secondary Firebox when a failover occurs.

Configuring High Availability

1 From Policy Manager, select **Network > High Availability**.
The High Availability dialog box appears.



2 Select the **Enable High Availability** check box.

3 Select the **HA1** check box for the interface to enable for High Availability.

4 In the **Primary Box IP** text box, you can change the default IP address. This IP address should be from a reserved or unassigned network. This becomes the permanent IP address for that interface.

5 In the **Secondary Box IP** text box, type an IP address from the same subnet as the interface with High Availability enabled on the active Firebox®.

6 Select the **HA2** check box to enable the HA2 interface.
The HA2 interface is optional.

7 Use the **Group ID** value control to identify this HA group on the network. If you use more than one HA pair on the same network, this number must be different for each pair.

8 Click the **Yes** radio button to encrypt all HA traffic between the Fireboxes. This is usually not necessary, and uses more resources.
or
Click the **No** radio button to not encrypt HA traffic between the Fireboxes.

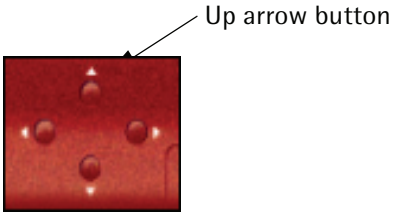
9 (If you selected the Yes radio button) In the **Shared Secret** field, type a shared secret to encrypt HA traffic between the Fireboxes. Type the shared secret again in the **Confirm** field.

10 Save this configuration to the active Firebox.

11 Close Policy Manager.

12 Use a crossover cable to connect the HA1 interface (eth5) on one Firebox to the HA1 interface on the other Firebox. If HA2 (eth4) is enabled, connect both HA2 interfaces as well.

13 Put the secondary unit in safe mode. To do this, turn the Firebox off, and then turn it back on while you hold down the up arrow button on the Firebox front panel.



14 Start Firebox System Manager and connect to the primary Firebox.

15 Select **Tools > High Availability > Synchronize Configuration**. When prompted, type the Read/Write passphrase.
You see a message that says High Availability is enabled.

Manually Controlling High Availability

Although High Availability operations usually occur automatically, you can do some of the functions manually.

Forcing a failover

You can cause a failover to occur. The standby system becomes the active one immediately.

From Firebox® System Manager, select **Tools > High Availability > Force Failover**.

Synchronizing the configuration

You must synchronize the configuration when one Firebox configuration changes while the other is disconnected from the HA peer or turned off.

From Firebox System Manager, select **Tools > High Availability > Synchronize Configuration**.

Restarting the peer

When you connect to an HA configuration, you communicate only to the active Firebox. To restart the peer Firebox, you must send the command from the active Firebox:

From Firebox System Manager, select **Tools > High Availability > Restart Peer**.

Note

When the Firebox is in a high CPU or traffic condition and you use Firebox System Manager to control HA operations, you can get an incorrect "time-out" message. In this case, the operation could have completed, and it is possible the time-out message is not correct.

Backing up an HA configuration

When a Firebox is in a High Availability pair, you can only back up the flash image of the Firebox when it is the active Firebox. This is because the backup image includes the system and policy information, certificates, and licenses that do not exist on the secondary Firebox until failover. To create a backup image (.fxi) of the active Firebox:

1 From Policy Manager, select **File > Backup.**

2 Type the configuration passphrase. Click **OK.**

3 Type and confirm an encryption key. This key is used to encrypt the backup file.
Type a strong encryption key that is easy to remember.

4 Browse or type the location for the backup file. Click **OK**.
The backup file is created.

5 Click **OK** when the backup is complete.

Upgrading Software in an HA Configuration

If you install the software on the active Firebox®, the standby Firebox in the HA configuration does not automatically upgrade. You must upgrade each Firebox. Upgrade the active Firebox first. When it restarts, the standby becomes the active Firebox. You can then upgrade that Firebox. You cannot upgrade the software on a Firebox that is in standby mode.

Using HA with Signature-based Security Services

Gateway AntiVirus for E-mail™ and Intrusion Prevention Service (IPS) signature databases do not automatically synchronize between active and standby HA devices.

If the antivirus and IPS features are enabled and an event occurs that causes the standby Firebox® to become active, this device can have a version of the AV and IPS signature databases that is not current (especially if it was in standby mode for a long time). Until an update of the database occurs, there is some time when a new virus or IPS attack can bypass the Firebox.

To minimize this problem, keep the automatic signature update intervals for Gateway AntiVirus for E-mail and Intrusion Prevention Service enabled and short. If possible, force a manual signature update on the new active Firebox immediately after the failover occurs.

Using HA with Proxy Sessions

When High Availability is activated with the default configuration, all outgoing TCP sessions are disconnected when a failover event occurs. Users must manually reestablish all interactive or persistant sessions. This is because proxy session state is not retained between HA peers, and the default configuration has a default TCP-proxy for all sessions. Packet filter sessions are maintained, but the packet filter is not used by default. Consider adding specific packet filter policies to your configuration for telnet, ssh, or any other policy for which you want failover. Note that IPS does not operate with these new policies.

CHAPTER 19

Configuring spamBlocker

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources.

The WatchGuard® spamBlocker™ option uses industry-leading pattern detection technology from Commtouch® to block spam at your Internet gateway and keep it from getting to your e-mail server. spamBlocker looks for patterns in spam attacks, instead of the contents of individual e-mail messages. Because it looks for content, it can detect spam in any language, format, or encoding method.

About spamBlocker

Before you install spamBlocker™, you must have:

- A spamBlocker license key certificate
- An SMTP e-mail server behind the Firebox®
- A SMTP Proxy policy
- Configured DNS on the Firebox.

spamBlocker actions

The Firebox uses spamBlocker actions to apply decisions about the delivery of an e-mail message that is spam. It can:

- **Deny** — Stop the spam message without a reply.
- **Tag** — Identify the message as spam or not spam and allow spam messages to go to the recipient. See the subsequent section for more information on spamBlocker tags.
- **Allow** — Let spam messages go through the Firebox without a tag.

spamBlocker tags

The Firebox can add spamBlocker tags to the subject line of the e-mail message. You can also configure spamBlocker to customize the tag that it adds. This example shows the subject line of an e-mail message that was found to be spam. The tag added is the default tag: ***SPAM***.

```
Subject: ***SPAM*** Free auto insurance quote
```

This example shows a custom tag: [SPAM]

```
Subject: [SPAM] You've been approved!
```

spamBlocker categories

spamBlocker looks at e-mail messages to find matches to the patterns in the spamBlocker database. It puts spam e-mail into three categories: Spam, Bulk, and Suspect. spamBlocker assigns e-mail messages to these categories based on the number of patterns found in the e-mail message.

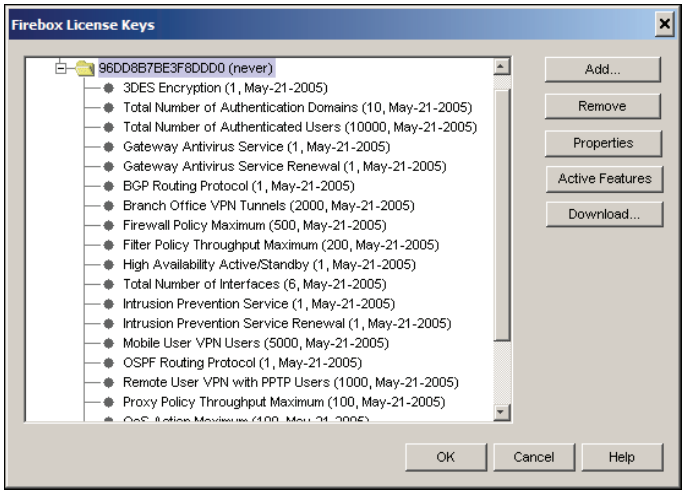
- The *Spam* category includes e-mail messages that come from known spammers. We recommend you use the Deny action for this type of e-mail.
- The *Bulk* category includes e-mail messages that do not come from known spammers, but do match some known spam structure patterns. We recommend that you use the Tag action for this type of e-mail.
- The *Suspect* category includes e-mail messages that look like e-mail messages that could be associated with a new spam attack. Frequently, these messages are legitimate e-mail messages. We recommend that you use the Allow action for this type of e-mail.

Installing the Software License

To install spamBlocker™, you must have a spamBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

To install this feature key:

1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.


Firebox License Keys
96DD8B7BE3F8DDD0 (never)
3DES Encryption (1, May-21-2005)
Total Number of Authentication Domains (10, May-21-2005)
Total Number of Authenticated Users (10000, May-21-2005)
Gateway Antivirus Service (1, May-21-2005)
Gateway Antivirus Service Renewal (1, May-21-2005)
BGP Routing Protocol (1, May-21-2005)
Branch Office VPN Tunnels (2000, May-21-2005)
Firewall Policy Maximum (500, May-21-2005)
Filter Policy Throughput Maximum (200, May-21-2005)
High Availability Active/Standby (1, May-21-2005)
Total Number of Interfaces (6, May-21-2005)
Intrusion Prevention Service (1, May-21-2005)
Intrusion Prevention Service Renewal (1, May-21-2005)
Mobile User VPN Users (5000, May-21-2005)
OSPF Routing Protocol (1, May-21-2005)
Remote User VPN with PPTP Users (1000, May-21-2005)
Proxy Policy Throughput Maximum (100, May-21-2005)
Add...
Remove
Properties
Active Features
Download...
OK
Cancel
Help

2 Click **Remove** to remove the current feature key.

3 Click **Add**.

4 In the **Add Firebox License Key** dialog box, type or paste your license key. You can click **Import** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

Activating spamBlocker

To activate spamBlocker™, you use a wizard that starts the feature and creates a basic configuration.

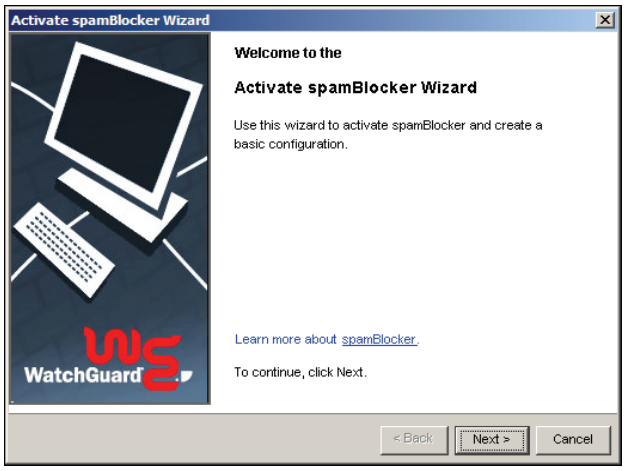
1 From WatchGuard System Manager, select the Firebox that will use spamBlocker.

2 Select **Tools > Policy Manager**.

Or,
you can click the Policy Manager icon on the WatchGuard System Manager toolbar.

3 From Policy Manager, select **Tasks** > **spamBlocker** > **Activate**.

The Activate spamBlocker wizard starts.



4 Click through the wizard and add the information it asks for. The wizard has these screens:

Apply spamBlocker settings to your policies

This screen appears if you already have one or more SMTP policies defined on your Firebox but do not have spamBlocker enabled. From the list, select the proxy policies for which you want to enable spamBlocker. Any policies that have spamBlocker already enabled are grayed out. If you do not have any SMTP policies defined at this time, this screen does not appear.

Create proxy policies

This screen appears if your Firebox does not yet have a policy created for SMTP. The wizard will create an SMTP proxy policy for you. You must have at least one external interface with a static IP address.

To create an SMTP policy, enter the e-mail server IP address. The policy created by this wizard contains "Any-External" for the **From** field and a static NAT entry for the **To** field. The static NAT entry uses the first static external IP address configured on the Firebox. It enables static NAT for the e-mail server IP address you enter in the wizard. If this default static NAT SMTP policy is not the best choice for your organization, you can use Policy Manager to create an SMTP policy before you use the wizard.

Select the spamBlocker actions

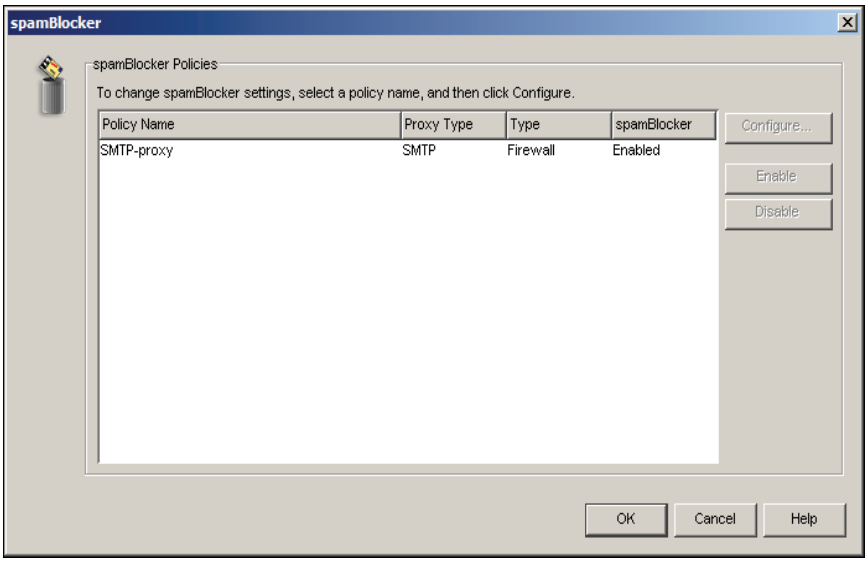
Use this screen to select the spamBlocker actions for e-mail in the Spam, Bulk, and Suspect categories.

If you want to record log messages for a spamBlocker response, select the **Log** check box. If you do not want to record log messages, clear the **Log** check box.

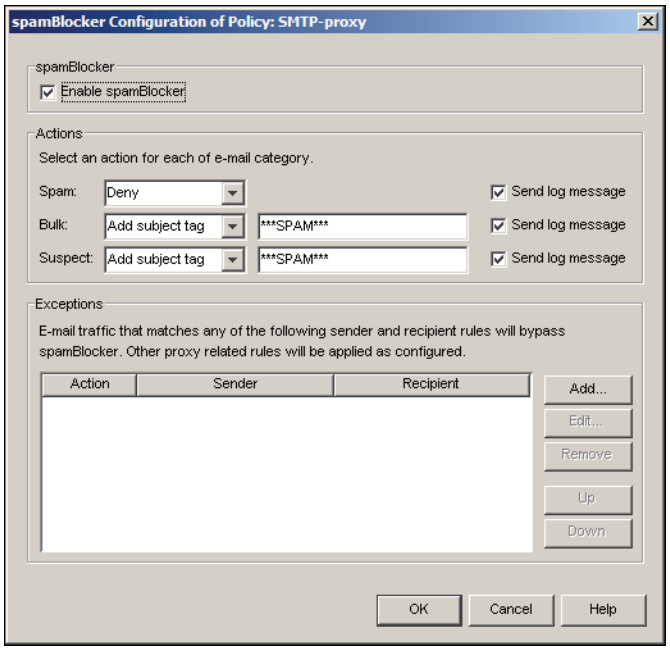
Configuring spamBlocker

After you use the Activate spamBlocker wizard to activate spamBlocker and create a basic configuration, you can set other configuration parameters.

1 From Policy Manager, select **Tasks** > **spamBlocker** > **Configure**.
The spamBlocker dialog box appears with SMTP policies in a list. It shows if spamBlocker is enabled for each policy.



2 Select the policy you want to configure and click **Configure**.
The spamBlocker Configuration page for that policy appears.



3 When you used the Activate spamBlocker wizard, you set the actions spamBlocker applies for e-mail in the Spam, Bulk, and Suspect categories. You can change the actions in this dialog box.

4 If you want to record log messages for a spamBlocker response, select the **Log** check box for the action. If you do not want to record log messages, clear the **Log** check box.

5 Make sure DNS is enabled on the Firebox that applies spamBlocker rules.

Note

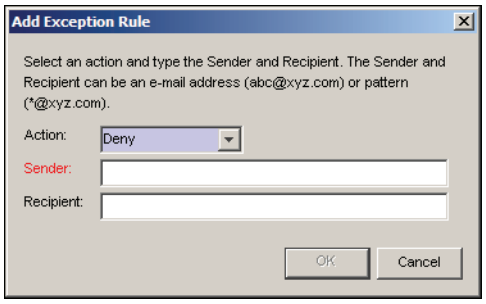
If you have any perimeter firewall between the Firebox that uses spamBlocker and the Internet, it must not block HTTP traffic.

Adding spamBlocker exceptions

At times, the Firebox identifies a message as spam when it is not spam. If you know the address of the sender, you can configure the Firebox with an exception after which it does not examine the messages from that source. To look for exceptions, spamBlocker looks at the “mail from:” field. It does not look at

the "From:" header that you see in e-mails. If you create an exception rule and it does not operate correctly, make sure you verify that you entered the correct field.

1 From the Exceptions block of the **spamBlocker Configuration** dialog box, click **Add**.
The Add Exception Rule dialog box appears.



2 Select a rule action: **Allow**, **Tag subject**, or **Deny**.

3 Type a sender, recipient, or both. You can type the full e-mail name or use wildcards.

Creating Rules for Bulk and Suspect E-mail on E-mail Clients

Many network administrators allow e-mail that is not confirmed as spam to be delivered to the destined e-mail recipient. They then set up rules in their e-mail client software to have any e-mail tagged as suspect or bulk e-mail put into a special folder on the e-mail client. The procedure below gives instructions on how to configure the Microsoft Outlook e-mail client. For information about how to use this procedure on other types of e-mail clients, look at the user documentation for those products.

Sending spam or bulk e-mail to special folders in Outlook

This procedure shows you the steps to create rules for bulk and suspect e-mail in Microsoft Outlook. You can have e-mail with a "spam" or "bulk" tag delivered directly to special folders in Outlook. When you create these folders, you keep possible spam e-mail out of your usual Outlook folders, but you can get access to the e-mail if it becomes necessary.

If you use another e-mail client, check your user documentation for that product.

Before you start, make sure that you set the action for spam and bulk e-mail to **Add Subject Tag**. You can use the default tags, or create custom tags. The steps below describe how to create folders with the default tags.

1 From your Outlook Inbox, select **Tools > Rules and Alerts**.

2 Click **New Rule** to start the Rules Wizard.

3 Select **Start from a blank rule**.

4 Select **Check messages when they arrive**. Click **Next**.

5 Select the condition check box: **when specific words in the subject**. Then, in the bottom pane, edit the rule description by clicking on the specific words. In the **Search Text** dialog box, type the spam tag as *****SPAM*****. If you use a custom tag, type it here instead. Click **Add**. Click **OK**.

6 Click **Next**.

7 The wizard asks what you want to do with the message. Select the **move it to the specified folder** check box. Then, in the bottom pane, click the word **specified** to select the destination folder.

8 In the **Choose a Folder** dialog box, click **New**. In the folder name field, type **Spam**. Click **OK**.

9 Click **Next** two times.

10 To complete the rule setup, type a name for your spam rule. Click **Finish**.

11 Click **Apply**.

12 Repeat these steps to create a rule for bulk e-mail, using the bulk e-mail tag. You can send bulk e-mail to the same folder, or create a separate folder for bulk e-mail.

Reporting False Positives and False Negatives

A false positive e-mail message is a legitimate message that spamBlocker™ incorrectly identifies as spam. A false negative e-mail message is a spam message that spamBlocker does not correctly identify as spam. If you find a false positive or false negative e-mail, you can report the classification error directly to Commtouch. You must have access to the e-mail message to submit the report. To learn how to submit a report for a false positive or false negative, go to:

https://www.watchguard.com/support/advancedfaqs/fw_spam-report.asp

Monitoring spamBlocker Activity

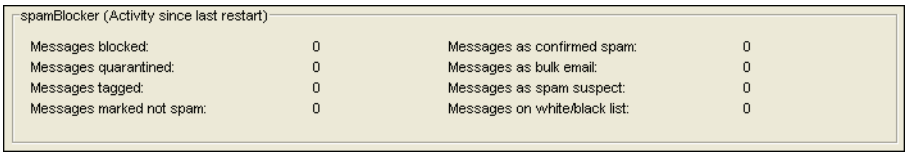
You can use Firebox System Manager to monitor spamBlocker™ activity.

1 From WatchGuard System Manager, select the Firebox whose spamBlocker activity you want to monitor.

2 Select **Tools > Firebox System Manager**.

Or,
you can click the Firebox System Manager icon on the WatchGuard System Manager toolbar.

3 From Firebox System Manager, click the **Security Services** tab.
The statistics for spamBlocker appear at the bottom of the screen.


spamBlocker (Activity since last restart)
Messages blocked: 0
Messages quarantined: 0
Messages tagged: 0
Messages marked not spam: 0
Messages as confirmed spam: 0
Messages as bulk email: 0
Messages as spam suspect: 0
Messages on white/black list: 0

Customizing spamBlocker using Multiple Proxies

You can configure more than one SMTP Proxy service to use spamBlocker™. This lets you create custom rules for different groups in an organization. For example, you can allow all e-mail to your management and use a spam tag for the marketing team.

If you want to use more than one SMTP Proxy service with spamBlocker, your network must use one of these configurations:

- Each user group must use a different e-mail server

or

- You must set the external source or sources that can send e-mail for each user group.

Note

spamBlocker does not detect spam in outbound SMTP e-mail.

APPENDIX A

Types of Policies

This chapter gives a list of the pre-defined policies included with Fireware Pro™ appliance software, their protocols, and their ports. It also gives special information about circumstances that could have an effect on the security of some policies.

In this chapter, policies are divided into two groups—policies that are controlled by a packet filter and policies that are controlled by a proxy.

Packet Filter Policies

Packet filter policies examine the source and destination headers of each packet. Packets are allowed or denied based on whether the headers appear to come from and go to trusted addresses.

Any

Use an Any policy only to allow all traffic between two specified trusted IP or network addresses. An Any policy opens a "hole" through the Firebox®, and allows all traffic to flow freely between specified hosts. We recommend that the Any policy be used only for traffic through a VPN.

The Any policy is different from other policies. For example, if you allow FTP only to a specified host, all other FTP sessions to other hosts are denied by that policy (unless you have also configured other FTP policies). The Any policy does not deny like other policies.

You also cannot use an Any policy unless specified IP addresses, network addresses, host aliases, group names, or user names are used in the **From** or **To** lists. If not, the Any policy does not operate.

Characteristics

- Internet Protocol(s): Any
- Port Number(s): Any port

AOL

The America Online proprietary protocol allows access to AOL through a TCP/IP network. The AOL client must be specially configured to use TCP/IP and not a modem.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 5190

archie

archie is a search protocol used to find files on FTP servers. We recommend that you use the available web interfaces to archie. A current list of archie servers is available through anonymous FTP from:

ftp://microlib.cc.utexas.edu/microlib/mac/info/archie-servers.txt

External hosts can be spoofed. The Firebox cannot make sure that these packets were sent from the correct location. You can configure your Firebox to add the source IP address to the Blocked Sites list when an incoming archie connection is denied. You can use all of the usual log options with archie.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 1525

auth

The Authentication Server protocol (AUTH) has a new name. It is now called the Identification Protocol (IDENT). Refer to IDENT for more information about this policy.

BGP

Border Gateway Protocol (BGP) is the routing protocol used across most of the Internet. It is a highly configurable protocol that can add redundancy to links to and from the Internet for LANs. We recommend that you use this service only if you have enabled and configured BGP in the dynamic routing processes in the Fireware configuration.

Characteristics

- Internet Protocol(s): TCP or UDP
- Port Number(s): 179

Citrix

Citrix, or Independent Computing Architecture (ICA), is an application protocol used by Citrix software applications such as Winframe and Metaframe Presentation Server (MPS). Winframe gives access to a Windows computer from different types of clients that use TCP port 1494. Citrix MPS 3.0 uses ICA with Session Reliability over TCP port 2598. If you use Citrix MPS, you must add a custom policy for TCP port 2598. If you add the Citrix policy, you could put your network security at risk because it allows remote access to computers through the firewall without authentication. The threat to a Winframe or MPS

server includes denial-of-service attacks. We recommend that you use VPN options to give more security for ICA connections. You can use all of the usual log options with WinFrame.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1494

For more information on how to add the Citrix ICA policy, refer to the Advanced FAQs in the Knowledge Base. Go to www.watchguard.com/support and log in to the LiveSecurity Service.

Clarent-gateway

Clarent Corporation supplies IP telephone technology to mainstream carriers and service providers. Clarent products allow voice-over-IP between Clarent gateways across the Internet. This policy gives support to the Clarent v3.0 product and later.

Clarent products use two sets of ports, one for gateway-to-gateway communications (UDP ports 4040, 4045, and 5010) and one for gateway-to-command center communications (UDP ports 5001 and 5002). Use the Clarent-command policy for the gateway-to-command center communications.

Allow incoming connections only from specified external gateways to your gateway or command center.

Clarent also gives support for the use of PCAnywhere for management. Refer to the PCAnywhere policy notes for more information.

The Clarent-gateway policy could put network security at risk because it allows traffic inside the firewall based only on network address. This is not a trusted method of authentication. In addition, your Clarent server could receive denial-of-service attacks in this configuration. Where possible, we recommend that you use VPN options to give more security for Clarent-gateway connections.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 4040, 4045, 5010

Clarent-command

Clarent Corporation supplies IP telephone technology to mainstream carriers and service providers. Clarent products allow voice-over-IP between Clarent gateways across the Internet. This policy gives support to the Clarent v3.0 product and later.

Clarent products use two sets of ports, one for gateway-to-gateway communications (UDP ports 4040, 4045, and 5010) and one for gateway-to-command center communications (UDP ports 5001 and 5002). Use the Clarent-command policy for the gateway-to-command center communications.

Allow incoming connections only from specified external gateways to your gateway or command center.

Clarent also gives support for the use of PCAnywhere for management. Refer to the PCAnywhere policy notes for more information.

The Clarent-command policy could put network security at risk because it allows traffic inside the firewall based only on network address. This is not a trusted method of authentication. In addition, your Clarent server could receive denial-of-service attacks in this configuration. Where possible, we recommend that you use VPN options to give more security for Clarent-command connections.

Characteristics:

- Internet Protocol(s): UDP
- Port Numbers(s): 5001, 5002

CU-SeeMe

CU-SeeMe is a software application used to do video conferencing through the Internet. For CU-SeeMe to operate through the Firebox, you must make sure that you are not on a network that uses outgoing dynamic NAT. Configure the CU-SeeMe policy for incoming and outgoing access.

The CU-SeeMe protocol makes you configure this policy for incoming and outgoing. The CU-SeeMe policy uses the correct ports to allow the use of CU-SeeMe versions 2.X and 3.X. CU-SeeMe Version 2.X operates on UDP port 7648. Version 3.X operates on UDP port 7648, UDP port 24032 (for H.323 conferences), and TCP port 7648 (video conference directories).

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Numbers(s): UDP 7648, UDP 24032, TCP 7648

DHCP-Server or DHCP-Client

Dynamic Host Configuration Protocol (DHCP) gives a way to allocate dynamic IP addresses to devices on a network.

Characteristics

- Internet Protocol(2): TCP
- DHCP-Server Port Number(s): 68
- DHCP-Client Port Number(s): 67

DNS

Domain Name Service (DNS) matches host names to IP addresses. A DNS policy is enabled in the default configuration. The DNS policy allows UDP DNS traffic, as well as TCP zone transfers to occur as specified. All of the usual log options can be used with DNS.

Characteristics

- Internet Protocol(s): Multi: TCP (for server-server zone transfers) and UDP (for client-server lookups)
- Port Number(s): TCP 53 and UDP 53

Entrust

The Entrust Authority Public Key distribution application protocol passes public keys to a trusted third-party organization for verification.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 709, 710

finger

finger is an application protocol used to get information about users on a given host. It is easy for a hacker to use this information against you. We do not recommend that you put finger servers on the trusted interface.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 79

FTP

File Transfer Protocol (FTP) is used to move files across the Internet. An FTP packet filter will not apply the FTP proxy rule set to any traffic. To proxy FTP traffic, use the FTP proxy policy. We recommend that incoming FTP be allowed only to public FTP servers located behind the Firebox.

External hosts can be spoofed. WatchGuard cannot verify that these packets were actually sent from the correct location. You can configure the Firebox to add the source IP address to the Blocked Sites list whenever an incoming FTP connection is denied. The packet filter and proxy policy included in WatchGuard Policy Manager handles the data channel for active and passive FTP sessions. All of the usual log options can be used with FTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): FTP uses two ports: TCP 20 for control connections and TCP 21 for data transfer. TCP 21 can be an incoming or outgoing connection depending on how the client is configured. If it is incoming, 21 is the source port, and the destination port is random.

Gopher

Gopher is a data-retrieval protocol developed at the University of Minnesota. Gopher is not frequently used, as most users use HTML.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 70, but servers can be configured to use other ports

GRE

Generic Routing Encapsulation Protocol (GRE) is used together with Point-to-Point Tunneling Protocol (PPTP) to create virtual private networks (VPNs) between clients or between clients and servers.

Characteristics

- Internet Protocol(s): GRE
- Protocol Number(s): 47

HTTP

A HTTP packet filter will not apply the HTTP proxy rule set to any traffic. To proxy HTTP traffic, use the HTTP proxy policy. We recommend that incoming HTTP be allowed only to public HTTP servers located behind the Firebox.

External hosts can be spoofed. WatchGuard cannot verify that these packets were actually sent from the correct location. You can configure the Firebox to add the source IP address to the Blocked Sites list whenever an incoming HTTP connection is denied. All of the usual log options can be used with HTTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 80

HTTPS

HTTPS is a secure and encrypted version of the HTTP protocol. The client and the web server set up an encrypted session on TCP port 443. Because this session is encrypted, the proxy cannot examine packet contents using a proxy. This policy uses a packet filter to examine the connection.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 443

HBCI

The Home Banking Computer Interface (HBCI) is a standard created for bank customers and manufacturers of banking products.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 3000

IDENT

The Identification Protocol (IDENT) is a protocol used to match TCP connections to a user name. It is used most frequently by large public SMTP and FTP servers. It is used for logs, but you cannot trust the information it gives, as attackers can change their servers to have them send back incorrect information. IDENT uses “fake” information to hide internal user information.

When you use SMTP with incoming static NAT, you must add IDENT to your Policy Manager. Configure IDENT to allow traffic to the Firebox. This enables mail messages to flow from behind the Firebox to the many SMTP servers on the Internet that use IDENT to identify other mail servers’ identities, and allows these servers to return messages through the Firebox to their senders.

If you are not using dynamic NAT, allow IDENT to the IP address of your e-mail server.

We recommend that IDENT policies be allowed to and from the Firebox, but know that hackers can use IDENT to collect user names.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 113

IGMP

The Internet Group Management Protocol (IGMP) is the standard for IP multicasting on the Internet. It is used to control host memberships in multicast groups on a single network.

Characteristics

- Internet Protocol(s): IGMP

IKE

The Internet Key Exchange Protocol is a standard protocol for key management.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 4500 and 500. UDP 4500 is used only for NAT traversal.

IMAP

Internet Mail Access Protocol (IMAP) is an application layer protocol for getting e-mail or bulletin board messages on a remote e-mail server as if the messages were local. You can get access to e-mail stored on an IMAP server from many locations (such as home, work, or laptop) without moving messages.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 143

IPSec

Internet Protocol Security (IPSec) is a framework for a set of protocols for security at the network or packet layer of network communications. It is a VPN tunneling protocol with encryption.

Characteristics

- Internet Protocol(s): UDP, encapsulated security payload (ESP), and authentication header (AH)
- Port Number(s): UDP 500 and UDP 4500

IRC

Internet Relay Chat (IRC) is a system for Internet chatting. To use IRC you must have an IRC client and Internet access. The IRC client is a software application on your computer that sends and receives messages to and from an IRC server. The IRC server makes sure that all messages are sent to all users in the chat session.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 6667

Intel Video Phone

Intel Video Phone is a real-time multimedia application based on H.323. H.323 is an international standard for conferencing over TCP/IP networks. This policy does not filter for dangerous content. It does not support QoS or rsvp protocol, and it does not support NAT.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1720, 522

Kerberos v 4 and Kerberos v 5

The Kerberos network authentication protocol is an authentication system developed by the Massachusetts Institute of Technology (MIT). Kerberos enables two computers to exchange private information across an open network using authentication for security.

Characteristics

- Internet Protocol(s): TCP and UDP
- Kerberos v 4 Port Numbers(s): UDP 750
- Kerberos v 5 Port Number(s): TCP 88 and UDP 88

L2TP

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate virtual private networks.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 1701

LDAP

Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for using online directory services. The protocol operates with Internet transport protocols, such as TCP. You can use LDAP to get access to stand-alone directory servers or X.500 directories.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 389

LDAP-SSL

Lightweight Directory Access Protocol over TLS/SSL (LDAP-SSL) is used with Windows 2000 to give more security when you access Active Directory.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 636

Lotus Notes

Lotus Notes is a client/server platform for conferencing, databases, e-mail. It is also used to create and use documents. This policy enables the proprietary Lotus Notes protocol. Because the protocol uses encapsulation and tunneling, and gives access to internal data, we do not recommend the Lotus Notes policy for addresses out of the trusted network.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1352, UDP 1352

MSSQL-Monitor

Microsoft SQL Monitor is used to monitor Microsoft SQL databases.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1434, UDP 1434

MSSQL-Server

Microsoft SQL Server is usually used to make a remote connection to a Microsoft SQL database.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 1433, UDP 1433

MS Win Media

Microsoft Windows Media Server is a proprietary protocol developed by Microsoft to supply unicast streams. It enables bidirectional connections that enable users to go forward, go back, or pause the playback of unicast streams.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1755, 80

NetMeeting

NetMeeting is a product developed by Microsoft Corporation that enables groups to teleconference across the Internet. It is included with Microsoft's Internet Explorer web browser. This policy is based on the H.323 protocol and does not filter for dangerous content. It does not support QoS or rsvp protocol, and it does not support NAT.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1720, 389

NFS

The Network File System (NFS) protocol is a client server software application created by Sun Microsystems to allow all network users to get access to shared files kept on computers of different types.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 2049, UDP 2049

NNTP

Network News Transfer Protocol (NNTP) is used to transmit Usenet news articles.

The best procedure to use NNTP is to set internal hosts to internal news servers and external hosts to news feeds. In most conditions NNTP must be enabled in two directions. If you operate a public newsfeed, you must allow NNTP connections from all external hosts. WatchGuard cannot make sure that these packets were sent from the correct location.

You can configure the Firebox to add the source IP address to the Blocked Sites list when an incoming NNTP connection is denied. All of the usual log options can be used with NNTP.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 119

NTP

Network Time Protocol (NTP) is a protocol built on TCP/IP that controls local timekeeping. It synchronizes computer clocks with other clocks located on the Internet.

Characteristics

- Internet Protocol(s): UDP and TCP

- Port Number(s): TCP 123 and UDP 123

OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for IP networks based on the link-state algorithm. OSPF is quickly replacing the use of RIP on the Internet because it gives smaller, more frequent updates to routing tables and makes networks more stable.

Characteristics

- Internet Protocol(s): OSPF
- Protocol Number(s): 89

pcAnywhere

pcAnywhere is a software application used to get remote access to Windows computers. To enable this protocol, add the PCAnywhere policy. Then, allow access from the hosts on the Internet that must get access to internal pcAnywhere servers, and to the internal pcAnywhere servers.

pcAnywhere is not a very secure policy and can put network security at risk, because it allows traffic through the firewall without authentication. Also, your pcAnywhere server can receive denial-of-service attacks. We recommend that you use VPN options to give more security.

Characteristics

- Internet Protocol(s): UDP and TCP
- Port Number(s): UDP 22, UDP 5632, TCP 5631, TCP 65301

ping

You can use ping to confirm whether a host can be found and is operating and on the network. To find DOS-based or Windows-based traceroute packets, configure a ping policy.

Outgoing ping is a good tool for troubleshooting. We do not recommend you enable ping connections incoming to your trusted network.

Characteristics

- Internet Protocol(s): ICMP
- Protocol Number(s): 1

POP2 and POP3

POP2 and POP3 (Post Office Protocol) are e-mail transport protocols, usually used to get a user's e-mail from a POP server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 109 (POP2), and 110 (POP3)

PPTP

PPTP is a VPN tunnel protocol with encryption. It uses one TCP port (for negotiation and authentication of a VPN connection) and one IP protocol (for data transfer) to connect the two peers in a VPN. Configure the PPTP policy to allow access from Internet hosts to an internal network PPTP server. PPTP cannot get access to hosts' static NAT because NAT cannot forward IP protocols. Because this policy enables a tunnel to the PPTP server and the Firebox cannot examine packets in the tunnel, use of this policy must be controlled. Be sure to use the most current version of PPTP.

Characteristics

- Internet Protocol(s): TCP
- PPTP Negotiation Port Number(s): 1723

RADIUS and RADIUS-RFC

The Remote Authentication Dial-In User Service (RADIUS) supplies remote users with secure access to corporate networks. RADIUS is a client-server system that keeps authentication information for users, remote access servers, and VPN gateways in a central user database that is available to all servers. Authentication for the network occurs from one location. RADIUS uses an authentication key that identifies an authentication request to the RADIUS client.

In RFC 2865, the server port used by RADIUS changed from port 1645 to 1812. Make sure you select the policy that matches your implementation.

Characteristics

- Internet Protocol(s): UDP
- RADIUS policy Port Number(s): UDP 1645
- RADIUS-RFC policy Port Number(s): UDP 1812

RADIUS-Accounting and RADIUS-ACCT-RFC

The Remote Authentication Dial-In User Service (RADIUS) Accounting policy supplies accounting information to administrators of networks that use RADIUS authentication. RADIUS is a client-server system that keeps authentication information for users, remote access servers, and VPN gateways in a central user database that is available to all servers. The RADIUS server is also notified when the authenticated session starts and stops. This information can be helpful for accounting.

In RFC 2866, the server port used by RADIUS changed from port 1646 to 1813. Make sure you select the policy that matches your implementation.

Characteristics

- Internet Protocol(s): TCP
- RADIUS-Accounting policy Port Number(s): UDP1646
- RADIUS-ACCT-RFC policy Port Number(s): UDP 1813

RDP

The Microsoft Remote Desktop Protocol (RDP) supplies remote display and input abilities over network connections for Windows software applications that operate on a server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 3389

RIP

Routing Information Protocol (RIP) is a link state routing protocol developed in the early years of routing. Its limitations make it inappropriate for use in the Internet, but it can be useful in small networks. We recommend that you use this service only if you have enabled and configured RIP in the dynamic routing processes in the Fireware configuration.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 520

RSH

Remote Shell (RSH) is used to get access to the command line of a remote host computer. Because it is not encrypted, we do not recommend you allow any RSH incoming through the Firebox without the use of a VPN.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 514

RealPlayer G2

Media streaming protocol v7 and v8.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 554, 80

Rlogin

Remote login (RLogin) is a UNIX command that allows an approved user to log in to other UNIX computers on a network. After the login, the user can do all the operations the host has approved, such as read, edit, or delete files. Because it does not use encryption, we recommend you do not allow incoming Rlogin through the Firebox.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 513

SecurID

RSA SecurID Two-Factor Authentication give more security to the user authentication procedure. Created by Security Dynamics Technologies, Inc., it uses SecurID tokens to generate codes and ACE/Server software to corroborate the codes.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 5510, UDP 5500

SMB (Windows Networking)

Windows uses Server Message Block (SMB) to share files, computers, printers, and other network resources.

If you set up replication, you can see many tries to use the port mapper service on port 135. When this fails, SMB begins to use port 42. Refer to the RFC for DCE, and the DCE-RPC proxy sections for more instructions.

Note

SMB through the Firebox is not secure and we do not recommend it, unless used through a VPN connection. These configuration settings are to be used only if there is no other alternative, and policy settings must specify internal and external hosts.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): UDP 137, UDP 138, TCP 139, TCP 445, UDP 445

SMTP

The SMTP packet filter policy allows SMTP traffic (e-mail) without using the SMTP proxy.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 25

SNMP

Simple Network Management Protocol (SNMP) is used to collect information about and configure remote computers. This can be dangerous. Many Internet attacks use SNMP. Because SNMP can cause changes in a network if enabled, carefully review alternatives and record logs for all connections.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 161

SNMP-Trap

Simple Network Management Protocol (SNMP) traps are notification messages that an SNMP agent (for example, a router) sends to a network management station. These messages usually report an important event that must be examined.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s):162

SQL*Net

Oracle uses one port for its sql*net software. By default, this port is 1526/tcp or port 1521/tcp. Or, edit the tnsnames.ora file to change the port. To allow sql*net through the Firebox, set up a policy for the port that your sql*net server uses, with a protocol of tcp, and a client port of ignore. Then set up incoming access from the allowed external hosts to the sql*net server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1521, 1526

SQL-Server

The SQL-Server policy is used to give access to Sybase Central and SQL Advantage software.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 10000

ssh

Secure Shell (ssh) is a free application protocol that allows remote login, command control, and the movement of files between computers. It gives strong authentication and secure (encrypted) connections. We recommend the use of ssh because it is more secure than more vulnerable protocols such as telnet, rssh, and rlogin.

UNIX versions are available from www.ssh.com, and information on versions for Windows can be found at F-Secure (http://www.f-secure.com).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 22

Sun RPC

Sun Remote Procedure Call (Sun RPC) was developed by Sun Microsystems for connections between clients and servers in the Sun network file system.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 111, UDP 111

syslog

syslog is a policy used to record operating system events on UNIX hosts. Syslog data is usually enabled on a firewall to collect data from a host outside the firewall.

The syslog port is blocked in the default Firebox configuration. To allow one log host to collect logs from more than one Firebox:

- Remove port 514 from the Blocked Ports list
- Add the WatchGuard Logging policy to Policy Manager

Note

It is usually not secure to allow syslog traffic through the Firebox. It is possible for hackers to fill syslogs with log entries. If the syslog is full, it is more difficult to see an attack. Also, the disk frequently fills up and the attack is not recorded.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 514

TACACS

TACACS user authentication is a system that uses user accounts to authenticate users into a dial-up modem pool. This removes the need to keep copies of accounts on a UNIX system. TACACS does not support TACACS+ or RADIUS.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 49

TACACS+

TACACS+ user authentication is a system that uses user accounts to authenticate users into a dial-up modem pool. This eliminates the need to keep copies of accounts on a UNIX system. TACAS+ supports RADIUS.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 49

TCP

This policy serves as the default policy for all TCP connections, and other policies override it. TCP connections that do not match specified policies in Policy Manager do not complete unless TCP-UDP, TCP, or

the TCP Proxy are also configured in Policy Manager. This policy does not enable FTP, which operates only with an FTP policy.

TCP-UDP

This policy serves as the default policy for all TCP and UDP connections, and other policies override it. Connections that do not match specified policies in Policy Manager do not complete unless TCP-UDP, TCP and UDP, or the TCP Proxy are also configured in Policy Manager. This policy does not enable active mode FTP, which operates only with an FTP policy.

UDP

This policy serves as the default policy for all UDP connections, and other policies override it. UDP connections that do not match specified policies in Policy Manager do not complete unless UDP, TCP-UDP, or the TCP Proxy are also configured in Policy Manager.

telnet

The telnet policy is used to log in to a remote computer. It is almost the same as dial-up access, but the connection is made across a network.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 23

Timbuktu

Timbuktu Pro is remote control and file transfer software used to get access to Windows computers. The protocol uses TCP port 1417 and UDP port 407. Add the Timbuktu policy and allow incoming access from the hosts on the Internet that must get access to internal Timbuktu servers, and to the internal Timbuktu servers.

Timbuktu is not a very secure software application and can put network security at risk. It allows traffic inside the firewall without authentication. In addition, the Timbuktu server can receive denial-of-service attacks. We recommend that you use VPN options for more security.

Characteristics

- Internet Protocol(s): TCP, UDP
- Port Number(s): UDP 407, TCP 1417

Time

The Time policy is almost the same as NTP. It is used to synchronize clocks between hosts on a network. Time is usually less accurate and less efficient than NTP across a WAN. We recommend that you use NTP.

Characteristics

- Internet Protocol(s): TCP, UDP

- Port Number(s): TCP 37, UDP 37

traceroute

traceroute is a software application that creates maps of networks. It is used for network troubleshooting, network route troubleshooting, and finding the Internet service provider of a site. The WatchGuard traceroute policy controls UNIX-based, UDP-style traceroute only. For a DOS-based or Windows-based traceroute packet filter, use the ping policy (see "ping" on page 42).

traceroute uses ICMP and UDP packets to create paths across networks. It uses the UDP TTL field to send back packets from each router and computer between a source and a destination. If you allow traceroute incoming to a network, this can enable a hacker to create a map of your private network. But, outgoing traceroute is good for troubleshooting.

Characteristics

- Internet Protocol(s): UDP
- Port Number(s): 33401-65535

UUCP

Unix-to-Unix Copy (UUCP) is a Unix tool and protocol that enables one computer to send files to another computer. This tool is not used frequently, as users more often use FTP, SMTP, and NNTP to transfer files.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 540

WAIS

Wide Area Information Services (WAIS) is a protocol you can use to find documents on the Internet. Thinking Machines Incorporated first developed WAIS. Some web sites use WAIS to look for searchable indices, but it is not used frequently.

WAIS is created on the ANSI Z39.50 search protocol, and the words Z39.50 and WAIS refer to the same technology.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 210, but servers can be (and frequently are) configured on other ports, much like HTTP servers

WinFrame

Citrix ICA is a protocol used by Citrix for its software applications, which includes the Winframe product. Winframe gives access to Windows from different types of clients. Citrix uses TCP port 1494 for its ICA protocol. Citrix MPS 3.0 uses Session Reliability by default. This changes the ICA protocol to use TCP 2598. If you use Citrix MPS, you must add a policy for TCP port 2598.

A WinFrame policy could put your network security at risk because it allows traffic through the firewall without authentication. In addition, your Winframe server can receive denial-of-service attacks. We recommend that you use VPN options to give more security for ICA connections. You can use all of the usual log options with WinFrame.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 1494

WG-Auth

The WatchGuard Authentication policy allows users to authenticate to the Firebox.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4100

WG-Firebox-Mgmt

The WatchGuard Firebox Management policy allows configuration and monitoring connections to be made to the Firebox. We recommend that you allow this policy only to the management station. The policy is usually set up on the trusted interface.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4103, 4105, 4117, 4118

WG-Logging

The WatchGuard Logging policy is necessary only if a second Firebox must get access to a log host on the trusted interface of a Firebox. If there is only one Firebox, this policy is not necessary.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4107, 4115

WG-Mgmt-Server

When you use the WatchGuard Management Server Setup wizard to configure a Management Server, the wizard automatically adds this policy to the gateway Firebox. It controls incoming connections to the Management Server.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 4110, 4112, 4113

WG-SmallOffice-Mgmt

The WatchGuard Small Office Management policy allows you to make a secure connection to SOHO and Edge Fireboxes from the WatchGuard Firebox System.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): TCP 4109

WG-WebBlocker

The WatchGuard WebBlocker policy allows connections to the WebBlocker server.

Characteristics

- Internet Protocol(s): TCP, UDP
- Port Number(s): TCP 5003, UDP 5003

whois

The whois protocol gives information about the administrator of web sites and networks. It is frequently used to find the administrator of a different web site.

To filter whois traffic, add a whois policy that allows connections to the whois server (such as rs.internic.net).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 43

X11

The X Windows System Protocol has components that are used to create graphic desktops, which include windows, colors, displays, and screens. X11 also supplies a flow of events that show the interaction between a user and a computer input device (such as a mouse, keyboard, and so on).

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 6000-6063

Yahoo Messenger

The Yahoo Messenger Protocol is a tool for instant messaging.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 5050, 80

Proxied Policies

This section reviews the proxied policies supplied by the WatchGuard® Firebox® System. A proxy policy opens packets, strips out forbidden data types in the packet content, and assembles the packets again using the source and destination headers of the proxy.

You configure and activate proxies the same way you add packet filtering policies.

DNS

Domain Name Service (DNS) matches host names to IP addresses. The DNS proxy policy examines the contents of DNS packets to help protect your DNS servers from hackers. It puts limits on the type of operations allowed in a DNS query and can look for specified patterns in query names.

Characteristics

- Internet Protocol(s): TCP and UDP
- Port Number(s): TCP 53 and UDP 53

FTP

FTP is File Transfer Protocol. FTP is used to move files across the Internet.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 20 (command channel), 21 (data channel)

HTTP

HTTP is the Hypertext Transfer Protocol used by the World Wide Web to move information around the Internet.

Note

The WatchGuard policy "HTTP Proxy" is not the same as an HTTP caching proxy. An HTTP caching proxy controls the caching of Web data. If you use an external caching proxy, you must enable (by adding policies) any outgoing policies that are necessary for your organization. If you do not, outgoing TCP connections do not operate correctly.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 80 (but servers can operate on any port, a common alternative is 8080, and Secure Socket Layer (SSL) connections are usually served on port 443)

SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet standard protocol used to transmit and receive e-mail. Usually SMTP servers are public servers.

You must add an auth policy to Policy Manager when you use incoming static NAT with SMTP (see "auth" on page 32). Configure auth to allow incoming auth to the Firebox. This enables outgoing mail

messages to flow freely from behind the Firebox to the many SMTP servers on the Internet that use auth. It allows these servers to send messages back through the Firebox to the senders.

Logging incoming SMTP is recommended, but this can cause a large quantity of logs. To not use the SMTP proxy but have SMTP operate correctly, create a new policy in Policy Manager that uses TCP protocol and port 25.

Characteristics

- Internet Protocol(s): TCP
- Port Number(s): 25

TCP Proxy

The TCP Proxy policy gives configuration options for HTTP on port 80 and adds a rule that allows TCP connections from networks behind the Firebox to networks external to the Firebox by default. The TCP Proxy rule makes sure that all HTTP traffic from behind the Firebox on all ports is proxied with the HTTP proxy rules.

We recommend that you allow HTTP only to any public HTTP servers kept behind the Firebox. External hosts can be spoofed. WatchGuard cannot make sure that these packets were sent from the correct location.

Configure WatchGuard to add the source IP address to the Blocked Sites list when an HTTP connection to a host behind your Firebox is denied. Configure the parameters and MIME types the same as you do for the HTTP Proxy.